U.S. ARMY DIGITIZATION MASTER PLAN

19960516 006

1 MARCH 1996

U.S. Army Digitization Office
DACS-ADO Rm# 2B683
200 Army Pentagon
Washington, D.C. 20310–0200
(703)-693-3300 DSN 223-3300 FAX (703)-693-4100
World Wide Web http://www.ado.army.mil

1. INTRODUCTION

1.1 Army Digitization Master Plan

1.1.1 Purpose

The *Army Digitization Master Plan (ADMP)* provides the roadmap for the introduction of digital information technologies as the Army transforms itself via the Force XXI process into a 21st Century force. The *ADMP* addresses strategies, responsibilities, requirements, architectures, acquisition, experimentation methodology, management processes, and coordination of digital battlespace issues in the Army, with the other Services, and within future coalition forces.

1.1.2 Scope

This annual update of the *ADMP* establishes the overall strategy for achieving battlespace digitization and defines the migration plans of individual battlespace systems to the Defense Information Infrastructure Common Operating Environment (DII COE). The Plan also describes how the Army is working toward achieving interoperability with joint and combined forces.

1.1.3 Objectives

The objective of the *ADMP* is to put forth a specific and measurable strategy for digitizing the battlespace. Individual objectives include:

- Identifying the primary partners in the process and delineating their responsibilities.
- Furnishing the framework for Army, joint, and multinational interoperability.
- Defining the Army's implementation strategy.
- Describing the digitization architectures.
- Detailing a streamlined acquisition strategy consistent with sound business practices and conforming to policies outlined in Department of Defense (DoD) Directive 5000.1.
- Laying out the process for evaluating and assessing system migrations to the DII COE.
- Highlighting the key support strategies and digitization issues.
- Depicting how the Army Digitization Office (ADO) will manage the integration of digital information and decision support systems within the joint and multinational arenas.
- Providing direction for future digitization efforts.

1.2 Force XXI Overview

The Army digitization effort is a vital part of the larger Army process for meeting the challenges of the 21st Century. Tomorrow's Army—Army XXI—will emanate from the reconceptualization and redesign of the force at all echelons, from the foxhole to the sustaining base. Assimilation of information and information technologies will be crucial to the success of this redesign effort.

1.2.1 Force XXI Campaign Plan

To achieve the objectives of Force XXI, the Army must change outmoded ways, retain essential values, and enhance warfighting capabilities to achieve decisive victory on future battlefields. The Force XXI Campaign Plan is the Army's means to identify outdated methods and propose new approaches. It incorporates three complementary and interactive efforts. The primary axis is focused on the redesign of the Army operational forces. The secondary axis is the redesign of the institutional forces—the elements that generate and sustain the operational forces. The final supporting axis is oriented on the development and acquisition of information age technologies, which are the overall enablers of the Force XXI Campaign. The Deputy Chief of Staff for Operations and Plans (DCSOPS) within Headquarters, Department of the Army (HQDA) is the executive agent responsible for coordinating the activities supporting the broad campaign.

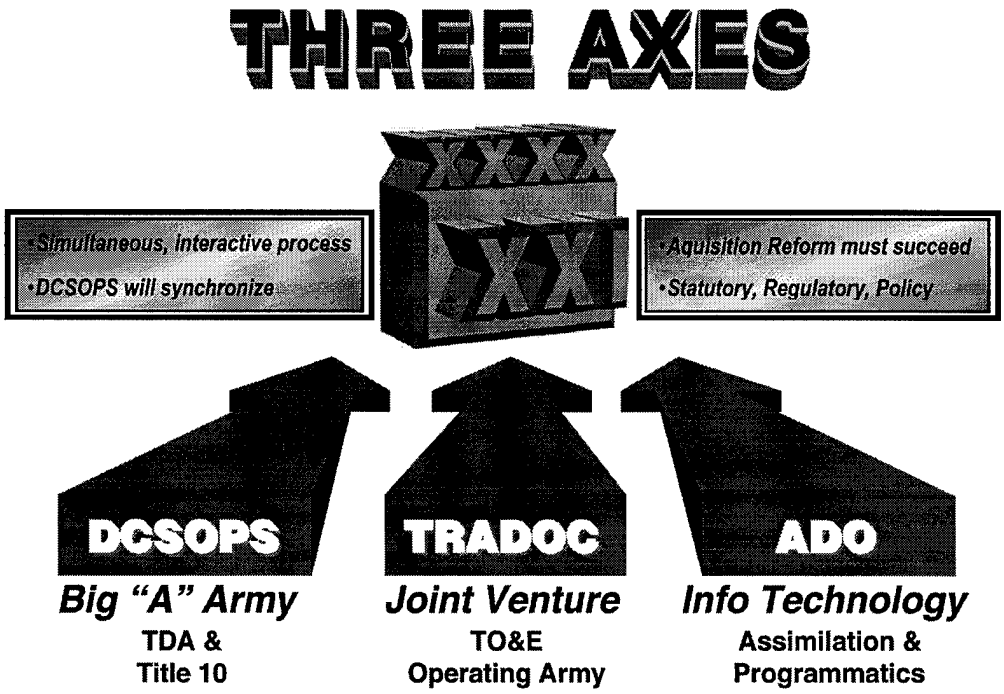


Figure 1-1 The Three Axes of the Force XXI Campaign

The central effort, designated *Joint Venture*, is led by the Commander, U.S. Army Training and Doctrine Command (TRADOC) in coordination with the other Army Major Commands (MACOMs) and the Army Staff (ARSTAF). It is intended to provide a framework to assess operational capabilities and determine how the Army will fight in the 21st century, while guiding development of doctrine, training, leader development, organizations, materiel, and soldiers

(DTLOMS). It also serves as the basis to develop the capability of Army forces to conduct successful operations under joint command employing modern, knowledge-based warfare. *Joint Venture* examines tactics, techniques, and procedures (TTPs) and technology alternatives that will enhance the lethality, survivability, and battle command capabilities of the operating forces.

The institutional effort, led by the DCSOPS, focuses on the concept, process, and design of the institutional Army and its sustaining base. This effort aims at continuous improvement to the organization to meet the continuing challenges of an uncertain world. Synchronization with the other two axes is necessary to ensure a seamless linkage from the foxhole to the factory.

The enabling effort, acquiring and assimilating information age capabilities, is led by the ADO. It provides for the introduction of modern information technologies throughout the force to optimize potential capabilities. It is to this effort that the term *digitization* is applied. The ADO balances and synchronizes requirements generated by TRADOC with technologies developed by the acquisition community to enable the Army to evolve into Army XXI.

The *ADMP* focuses on the execution of the ADO axis. Iterative cycles of experimenting, learning, and deciding between competing modernization initiatives characterize the execution process, with streamlined acquisition procedures allowing more rapid implementation of decisions.

1.2.2 Horizontal Technology Integration (HTI)

HTI is a key component of the Army Modernization Strategy, oriented on system upgrades that capitalize on new technology insertion, rather than developing new system platforms. There are currently four HTI initiatives: digitization, the Battlefield Combat Identification System (BCIS), the Second Generation Forward Looking Infra-Red (2nd Gen FLIR) system, and the Suite of Survivability Enhancement Systems (SSES)

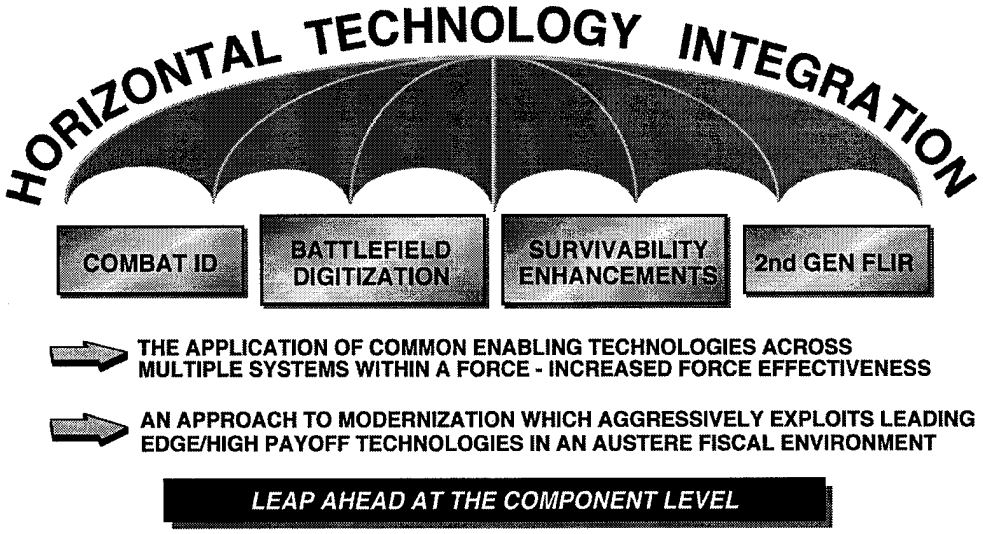


Figure 1-2 HTI Modernization Efforts

HTI breaks away from traditional stovepipe processes of individual systems and looks instead at the interaction of systems within the force. It integrates dissimilar weapons and command and control platforms with common technologies through new acquisition and fielding, pre-planned product improvements (P3I), and system-component upgrades. Simultaneously integrating complementary HTI technologies into key combat, combat support, and combat service support (CSS) systems increases effective combat power much sooner, in contrast to the old manner of sequential upgrades throughout the entire force. HTI increases the combat power of the Army one unit at a time with priority given to the contingency forces—the first to be deployed.

The *ADMP* addresses the ADO strategy to implement HTI's digitization objectives. BCIS and 2nd Gen FLIR, while not a part of the digitization effort, are closely monitored to ensure the necessary linkages for generated data are maintained and redundancies eliminated.

1.2.3 Battlefield Visualization

Another key component of Force XXI is *battlefield visualization*. This is the process whereby the commander develops a clear understanding of the current state with relation to the enemy and environment, envisions a desired end state which represents mission accomplishment, and then subsequently visualizes the sequence of activity that moves the commander's force from its current state to the end state.

Intuition, training, and experience—coupled with digital technology—will enable commanders to visualize the operation, formulate and analyze friendly and enemy courses of action, develop and communicate their intent, and monitor the operation to ensure conformance. Digitization will provide the tools to allow the commander to visualize and assess the sequence of actions during the battle in near real-time. An integrated battle command and decision support system will assist the commander in mission planning, facilitate effective rehearsals, and validate the understanding of the commander's intent prior to initiation and throughout the execution of the mission.

Digitization will make possible a high degree of *total mission awareness* at all echelons. It will begin with friendly force *situational awareness* brought about by the digitization of key platforms and soldiers in the battle area, providing leaders with near real-time information on current unit positions and their tactical/logistical status. Intelligence sources that feed into the battle command system—ranging from advanced sensors to soldier spot reports—will enable a continuous tracking of enemy locations and an intelligently derived and widely disseminated analysis of probable enemy intent. The ensuing *relevant common picture* derived from distributed databases can be tailored for resolution and content by the appropriate level of command. The databases themselves must be able to be exchanged, accessed, and shared at the appropriate level among all agencies involved in the operation.

Battlefield visualization management and campaign plan issues are being addressed through battlefield visualization working groups, chaired by the Force Development Directorate, DCSOPS, HQDA, at both action officer and general officer levels.

1.3 Digitization of the Battlespace

1.3.1 Vision

Digitization is the essential enabler that will facilitate the Army of the 21st Century's ability to win the information war and provide deciders, shooters, and supporters the information each needs to make the vital decisions necessary to overwhelm and overcome their adversary and win the final campaign.

1.3.2 Definition

Digitizing the battlespace is the application of information technologies to acquire, exchange, and employ timely information throughout the battlespace, tailored to the needs of each decider (commander), shooter, and supporter, allowing each to maintain the clear and accurate vision of the battlespace necessary to support mission planning and execution.

Digitization allows the warfighter to communicate vital battlefield information instantly, rather than through slow voice radio and even slower liaison efforts. It provides the warfighter with a horizontally and vertically integrated digital information network that supports unity of battlefield fire and maneuver and assures command and control decision-cycle superiority. The intent is to create a simultaneous, appropriate picture of the battlespace at each echelon—from soldier to commander—based on common data collected through networks of sensors, command posts, processors, and weapon platforms. This allows participants to aggregate relevant information and maintain an up-to-date awareness of what is happening around them.

1.3.3 Requirements

The broad conceptual and requirements-driven underpinnings upon which digitization is built are documented in the *Horizontal Integration of Battle Command (HIBC) Mission Need Statement (MNS)*. The *HIBC MNS* establishes the baseline operational requirements for digitization of the battlespace and future command systems.

It was approved by the Department of the Army and forwarded to the Joint Requirements Oversight Council (JROC) for validation in October 1994. The Defense Information Systems Agency (DISA) and the Joint Staff (J6) granted Command, Control, Communications, and Computers (C4) interoperability certification on 6 December 1994. The MNS was subsequently validated by the JROC on 10 January 1995. MNS validation was required for expenditure of Research, Development, Test, and Evaluation (RDTE) funds for digitization in support of Advanced Warfighting Experiments (AWEs).

The operational baseline provides for:

- The capability to react on information faster than the enemy.
- Enhanced situational awareness at all levels.

- Rapid processing and transfer of information.

- An increased ability to synchronize direct and indirect fires.

- A means to establish and maintain an overwhelming operational tempo.

The general capabilities required by the *HIBC MNS* are grouped within five broad categories:

- **Battle command.** Integrate battle command functionality within and among weapons systems, command posts, sensors, and support systems. Develop linkages between discrete systems. Achieve horizontal integration between Battlefield Functional Areas (BFAs) and vertical integration between tactical and operational levels. Incorporate automatic exchange of digital information and electronic transmission of maps, overlays, and orders.

- **Common picture**. Endow commanders at all echelons with the ability to maintain a clear picture of their relevant battlespace with an enhanced level of situational awareness. Reduce fratricide by furnishing a supplemental means to identify friend or foe. Supply faster, more comprehensive access to intelligence data with near real-time fusion and dissemination of the intelligence picture via a common database enabling rapid information transfer.

- **Lethality/survivability**. Merge state-of-the-art information technology into battle command systems. This will facilitate the concentration of combat power by means other than traditional massing of forces, while enabling units to be more survivable and lethal. Related capabilities include rapid acquisition, correlation, and communication of target data to weapons platforms and automated target hand-off among close combat ground, air, and fire support systems.

- **Logistics**. Rapidly determine, communicate, and respond to logistics support requirements for tailored, specialized fighting units during split-based contingency operations. Information technologies must substantially improve the capability to request, assemble, and transport vital resources from the sustaining base to forward operating locations.

- **Joint interoperability**. Seamlessly interface a multi-layered battle command system with the joint Global Command and Control System (GCCS) at the appropriate echelons. It must be interoperable with joint Command, Control, Communications, Computers, and Intelligence (C4I) programs and DII COE-compliant programs of other Services, employing common technologies and procedures where feasible.

The *HIBC MNS* does not describe a materiel solution, but does establish the following series of basic hardware and software constraints:

- Standardized hardware to reduce costs and simplify maintenance.

- Use of modularity and an open architecture to facilitate ease of upgrades.

- Option of embedded or applique hardware—as appropriate to the system.
- Mix of commercial off-the-shelf (COTS), ruggedized, and mil-spec components.
- Technical architecture consisting of common applications, standards, and protocols.
- User-friendly interface, permitting effective operation in a tactical field environment.
- Standard Defense Mapping Agency (DMA) digital map and terrain data, as well as hasty data provided by Army topographic elements.
- Common graphics and tactical symbology.
- Command and control able to support operations on-the-move with minimal degradation.
- Equipment able to operate in the same environmental conditions as the host platforms.
- Means to identify friend, foe, or noncombatant using sensor and/or data sources.
- Standard C4I systems meeting DII COE interoperability and interface requirements.

General capabilities are tailored to allow the smaller force projection Army to concentrate combat power *effects* efficiently and decisively, rather than physically massing forces and firepower by traditional means. The intent is to enable contingency forces—comprised of fewer and smaller units—to be more lethal and survivable in an environment characterized by an accelerated operational tempo demanding instant communications and immediate response times. As requirements are refined through the experimental process, formal requirements documents providing more detailed guidance to system developers will be published.

1.3.3.1 Operational Requirements Documents

The *Army Battle Command System: Common Operating Environment/Common Applications Operational Requirements Document (ABCS: COE/CA ORD)* will further refine the operating capability needs defined in the *HIBC MNS*. This document, developed by TRADOC, calls for the migration of separate Army command and control component systems into one integrated system. The *ABCS: COE/CA ORD* was forwarded to DCSOPS, HQDA for staffing in August 1995.

The *Force XXI Battle Command, Brigade-and-below (FBCB2) ORD* defines the needed command and control capabilities down to the lowest echelons. TRADOC delivered the ORD to HQDA for initial staffing in June 1995. It will be refined and updated by TRADOC at the conclusion of the Task Force (TF) XXI AWE, after which it will be resubmitted for final coordination and approval.

1.3.4 Army Digitization Rules

The plan to accomplish the required tests and experiments is ambitious and involves many diverse organizations and potentially conflicting interests. To clarify the process and simplify the procedures, the ADO has established five basic rules for participation:

- **Rule 1**: Army agencies which require a command and control (C2) applique solution for their experiments, materiel developments, or operational needs are restricted to using one of the three versions of applique hardware available under the Program Executive Officer for Command, Control, and Communications Systems (PEO C3S) applique contract. No other unique prototypes/models may be used.

- **Rule 2**: PEO C3S, as the executive agent for the ADO, will utilize the user jury process to provide a forum to make decisions on software and hardware capabilities that are candidates for Force XXI events. The user jury will also evaluate screen designs and software functions that will be incorporated into programs which are required to implement common battle command functions. The user jury process is the primary means through which the Army will identify and document new functionality to be included in FBCB2. Agencies with prototype battle command systems or good ideas for new applications will submit them to the user jury and not independently market them to other agencies or units.

- **Rule 3**: Part of the Army Technical Architecture (ATA) is the Technical Interface Design Plan for K–series Variable Message Formats (VMF), which describes specific requirements for information exchange. VMF messages must be implemented in all Army platforms operating in the brigade-and-below battlespace. The Army is coordinating these message formats with the other Services and the Joint Interoperability Engineering Organization (JIEO) to obtain approval for joint implementation.

- **Rule 4**: All future contracts for new system developments, Advanced Technology Demonstrations (ATDs), Advanced Concepts Technology Demonstrations (ACTDs), Advanced Concepts in Technology II (ACT II) programs, or modification to existing systems will require conformance to the ATA and the use of the DII COE for hosting of any and all command and control–related systems or subsystems. All contracts for brigade-and-below systems—whether new system developments, ATDs, ACTDs, ACT II programs, or modification to existing systems—which will use or exchange data with Single Channel Ground and Airborne Radio Systems (SINCGARS)–equipped systems must support the SINCGARS System Improvement Program (SIP) waveform, MIL STD 188-220A, VMF, and MIL STD 2045-14502.

- **Rule 5**: Waivers from or modification to the above rules must be approved by the ADO.

1.3.5 Goals

The major goals of Army digitization include the following:

- Acquiring and fielding a near-term FBCB2 system.

- Establishing a *Tactical Internet.*
- Conducting AWEs to evaluate the benefits and progress of digitization efforts.
- Digitally integrating the Battlefield Operating Systems (BOS).
- Developing a Battlefield Information Transmission System (BITS).
- Fielding digitized Force XXI weapons systems.

These goals include both near-term and far-term objectives. Each objective carries a dissimilar risk level and will require different focus and attention as digitization progresses over time.

1.4 Army Digitization Office (ADO)

The ADO is the primary coordinating and synchronizing organization in the process of developing and fielding digitization capabilities. It acts as a conduit for streamlining the materiel acquisition process, and provides new opportunities for industry to participate in Army programs. The Army research and development commands, as executive agents for the ADO, perform the actual research, development and acquisition functions.

1.4.1 Historical Basis

The HQDA Digitization Special Task Force (STF) was formed in January 1994 to clarify the Army's digitization goals. It developed the initial digitization strategy and created the nucleus of the ADO. Established in July 1994, the ADO oversees and coordinates the integration of Army digitization activities. The ADO's extended membership includes doctrinal developers, training developers, technical experts, procurement officials, and representatives working together with industry to capitalize on emerging information-age technology.

1.4.2 Mission

The ADO mission is to:

- Oversee the coordination and integration of the Army battlespace digitization activities.
- Advise the Army Acquisition Executive (AAE) and Vice Chief of Staff, Army (VCSA) on all matters concerning the integration of digital capabilities across the force and oversee the integration of Army digitization activities consistent with guidance from the AAE, VCSA, and Chief of Staff, Army (CSA).
- Oversee and coordinate the implementation of the *ADMP* with the support of appropriate MACOMs and supporting agencies.
- Advocate and support streamlined acquisition strategies to develop, assess, procure, and field equipment in support of the aggressive Force XXI timelines.

- Oversee digitization integration through a Management Decision Package (MDEP).

1.4.3 Organization and Responsibilities

The ADO is organized into four functional teams to accomplish its assigned mission and objectives, as shown in Figure 3.

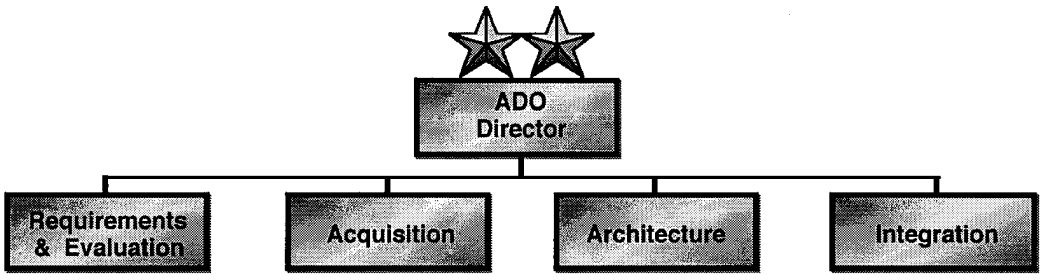


Figure 1-3 ADO Organization

1.4.3.1 Requirements and Evaluation Team

The Requirements and Evaluation Team supports the Army digitization axis by coordinating user requirements, test, evaluation, and experimentation issues. This process involves liaison with TRADOC, the Experimental Force (EXFOR), and the ARSTAF to define and resource user requirements. The team then coordinates with materiel developers, combat developers, and the test and evaluation community to validate hardware and software candidates identified to satisfy those needs. The team is responsible for supporting the *Joint Venture* axis of the *Force XXI Campaign Plan* by monitoring and coordinating battle command digitization issues for the Task Force XXI, Division XXI, and Corps XXI AWEs and supporting exercises.

Specifically, the team is responsible for monitoring the development and approval of requirements documents that impact battlespace digitization. The team is the ADO's point of contact for all requirements documents affecting the Army digitization effort.

The Requirements and Evaluation Team also interfaces with the test and evaluation community to ensure sufficient analytic rigor exists to justify procurement decisions. This requires close coordination with TRADOC to determine the important operational performance objectives are in each AWE. The team represents the ADO on the Analysis and Experimentation Planning Group (AEPG), which is responsible for developing a coordinated, consolidated evaluation plan for major experiments. The team also assists in the development of the digitization *Experimentation Master Plan (EXMP),* a document similar to a Test and Evaluation Master Plan (TEMP), which articulates the methodology to meet TF XXI AWE objectives. The *EXMP* will be updated after the TF XXI AWE to reflect remaining issues to be addressed in the Division and Corps XXI AWEs, as well as

those emanating from Battle Lab Warfighting Experiments (BLWEs). The team is also involved with other plans, such as the *Tactical Internet Experimental Plan.*

An additional area of responsibility is integration of modeling and simulation into the analytical and experimentation framework. The team monitors the on–going development of the Synthetic Theater of War (STOW) and ensures upgrades are made to existing command, control, and communications models/simulations (C3 M/S).

Other areas of involvement include participation in various Force XXI Process Action Team (PAT) meetings for AWEs, synchronization meetings chaired by DCSOPS, C3I M/S conferences, and Distributed Interactive Simulation (DIS) standards committees. The team also monitors Battle Lab digitization initiatives and availability of modernized and digital equipment provided to the EXFOR.

1.4.3.2 Architecture Team

The Architecture Team serves as the focal point for all digitization technical efforts and coordinates technical issues with the Director of Information Systems for Command, Control, Communications, and Computers (DISC4), PEOs, Army Materiel Command (AMC), Space and Strategic Defense Command, Ballistic Missile Defense Organization, Army Medical Command, and materiel developers from the Marine Corps, Navy, and Air Force. The team has sufficient technical expertise to provide the Army Secretariat with independent technical assessments of digitization issues.

The Architecture Team is specifically responsible for ensuring that the development and implementation of the System and Operational Architectures conform to the Army Technical Architecture. The team actively works with the DISC4 and the Army Systems Engineering Office (ASEO) to coordinate and review the continued development of the ATA. The team reviews the Technical Architecture to ensure commercial standards and practices are used in the development of common protocols and standards, and that the Army is represented in military and commercial standards bodies. The team also makes recommendations to the appropriate agencies for enforcing the application of the Technical Architecture in all related digitization projects, to include embedded digital systems such as the M1A2 tank and the AH-64D helicopter.

The team works with the Signal Center, PEO C3S, and the Communications and Electronics Command (CECOM) to plan for the development of the *Tactical Internet* and the evolution to BITS. The team's efforts include analyzing data and conclusions from modeling conducted by the Signal Center and PEO C3S, reviewing System Architecture specifications, and ensuring that adequate system integration and testing is performed before equipment is provided to the EXFOR.

The Architecture Team is also responsible for ensuring that sound system engineering practices are being followed, to include hardware and software configuration control, creation of a *Systems Engineering Management Plan*, and the conduct of Preliminary and Critical Design Reviews.

1.4.3.3 Acquisition Team

The Acquisition Team is responsible for resource management, acquisition planning oversight, and the streamlining of the acquisition process in support of the Force XXI digitization effort. It recommends, maintains, and updates planned digitization program funding by use of a digitization MDEP, and manages the program execution of its own budget lines. The team ensures that funding outlined in the MDEP is programmed, budgeted, and executed in a manner consistent with the *ADMP* and established Army priorities. In addition, the Acquisition Team coordinates the MDEP with the ARSTAF, MACOMs, PEOs, and Program Managers (PMs). The results are briefed to the AAE and VCSA. The PEOs/PMs must inform the ADO when resource allocation adjustments occur within the MDEP. In a collaborative effort, the ADO, MACOMs, and PEOs/PMs recommend adjustments to the MDEP which best meet the needs of the Army's digitization effort. The MDEP includes funding for various Research and Development (R&D) Program Elements (PEs) and procurement Standard Study Numbers (SSNs) related to digitization.

The Acquisition Team will periodically conduct technical and program execution reviews on all key contracts directly related to Force XXI digitization. PEOs/PMs will provide copies of status reports to the ADO in the same format and frequency as required by their higher headquarters.

The team's Acquisition Strategy for digitization will incorporate a streamlined approach characterized by an intense management of resources at all levels. Close coordination with TRADOC and materiel developers will ensure timely responses to user needs through appropriate adjustments to acquisition plans and procurement actions. Examples of this streamlined acquisition approach include identification of commercial non-developmental item (NDI) options, maximum consideration of commercial standards and practices, and leveraging of ongoing acquisitions by participating platform managers.

The Acquisition Team also provides, budgetary, programmatic, contractual, and logistics support to the ADO.

1.4.3.4 Integration Team

As the operations cell for the ADO, the Integration Team is responsible for coordination of Army digitization policy and strategy. It also serves as the principal integrator of digitization policies within the Army and coordinates with agencies external to the Army.

Within the Army, the Integration Team coordinates digitization strategy with DCSOPS and MACOMs in support of the Force XXI modernization effort. It serves as the primary interface on digitization policy and strategy matters with the Army Secretariat, ARSTAF, MACOMs and Army agencies. The team also coordinates integration of digital capabilities within ATDs and AWEs.

External to the Army, the Integration Team is the primary coordinating arm for the ADO on all matters concerning joint and multinational digitization strategy and policy. It also prepares Congressional correspondence, digitization briefings, and organizes conferences for the Director.

With respect to industry, the Integration Team investigates proposed Battle Lab and commercial technologies that may have an impact on the digitization effort. It also provides information to industry on the major thrusts of digitization.

The Integration Team compiles and maintains a list of all issues/requirements identified as part of the digitization process. As issues are identified, they are added to the issue tracking process and followed until resolved. In addition to internal Army processes, the team participates in several joint fora, such as the Military Communications and Electronics Board (MCEB). Any issues relating to joint matters are surfaced in this forum, with issues evaluated, prioritized, and assigned to an organization or agency for resolution. The team verifies that identified issues are being adequately addressed and resolved.

Finally, the Integration Team creates and maintains policy documents. Most important of these documents is the *ADMP,* which provides the roadmap for future Army digitization efforts. The Integration Team also coordinates the Digitization Master Schedule, which integrates the schedules of major Army systems and technologies that have a direct impact on the digitization of Army XXI. The current version of this schedule is available on the ADO Home Page (http://www.ado.army.mil).

THIS PAGE INTENTIONALLY LEFT BLANK

2. RESPONSIBILITIES

The technical nature and aggressive timelines associated with Army digitization efforts require the coordinated actions of all agencies involved to successfully accomplish the Force XXI modernization objectives. The following is a listing of the primary partners in this process and their responsibilities related to digitization:

2.1 Assistant Secretary of the Army for Research, Development and Acquisition/Army Acquisition Executive (ASA(RDA)/AAE)

ASA(RDA)/AAE is responsible for:

- Sponsoring ATDs that bring digital capabilities to a state of technical maturity and demonstrate their military utility before incorporation into follow-on BLWEs and AWEs.
- Providing planning, authorization, and funding support for Force XXI requirements.
- Serving as the Army Technical Architect.
- Coordinating digitization science and technology (S&T) efforts with the Advanced Research Projects Agency (ARPA).
- Ensuring that digitization efforts capitalize on acquisition streamlining initiatives.
- Providing appropriate M/S support.
- Coordinating technical architecture (TA) and S&T efforts with joint and DoD C4I Component Acquisition Executives (CAEs).

2.2 Deputy Chief of Staff for Personnel (DCSPER), HQDA

DCSPER is responsible for ensuring that properly qualified soldiers are recruited, trained, assigned, and retained to meet the skill requirements of the digital battlefield.

2.3 Deputy Chief of Staff for Intelligence (DCSINT), HQDA

DCSINT is responsible for:

- Coordinating signal, human, imagery, measurements, and signature intelligence programs and the counterintelligence and security countermeasures activities supporting the digitized battlefield.
- Establishing priorities for expanding and maintaining the digital terrain database.
- Coordinating security-related policy changes required for digitization efforts.

2.4 Deputy Chief of Staff for Operations and Plans (DCSOPS), HQDA

DCSOPS is responsible for:

- Integrating and synchronizing all efforts across the three axes of the *Force XXI Campaign Plan*, and leading the axis to re-engineer the Table of Distribution and Allowances (TDA)/Institutional Army in concert with Army commanders.
- Adjusting the fielding schedules of programs—such as Army Tactical Command and Control Systems (ATCCS) and tactical radio communications systems—as needed to support AWE train–up and execution schedules.
- Ensuring digitization programs are prioritized and resourced consistent with the CSA's goals and timelines associated with fielding a digitized Army XXI.
- Overseeing and validating the Operational Architecture (OA) developed by TRADOC.
- Coordinating Land Information Warfare activities.
- Maintaining the *Force XXI Campaign Plan.*
- Providing appropriate M/S support.

2.5 Deputy Chief of Staff for Logistics, (DCSLOG), HQDA

DCSLOG is responsible for providing a seamless logistics system which is flexible, deployable, tailorable, and integratable into the digitized battlespace.

2.6 Chief of Engineers (OCE-P), HQDA

OCE-P is responsible for maintaining the digital terrain database.

2.7 Director of Information Systems for Command, Control, Communications, and Computers (DISC4), HQDA

DISC4 is responsible for:

- Providing oversight and proponency for the *Army Enterprise Strategy* and ensuring that the strategy is executable, compatible, and consistent with Army guidance and direction.
- Supporting the AAE by developing and updating the ATA with the support of the ARSTAF, PEOs, MACOMs, and agencies.
- Exercising spectrum management responsibilities in support of digitization efforts.
- Overseeing the employment of Communication Security (COMSEC) devices in the System Architecture (SA).

- Overseeing and coordinating the implementation of Army software reuse policy in support of digitization efforts.

- Orchestrating the development of the *Command and Control Protect* program in coordination with DCSOPS and DCSINT.

- Addressing and resolving integration security issues.

- Coordinating the Army's Operational, Technical, and System architectures with the Office of the Secretary of Defense (OSD) and the other Services.

- Providing appropriate M/S support.

- Overseeing development, programming, and funding for BITS.

- Overseeing data standardization efforts for the Army while retaining the capability to interface with joint systems.

2.8 Army Digitization Office (ADO), HQDA

ADO is responsible for:

- Integrating and synchronizing Army digitization efforts.

- Providing guidance, assistance, and direction in acquisition matters related to digitization.

- Planning, programming, and budgeting for all applique-related costs. These include: applique procurement; installation kit procurement and installation; system engineering; hardware and software changes resulting from the Task Force XXI and Division XXI experiments; and the development and maintenance of the FBCB2 software module for embedded systems.

- Recommending and applying streamlined acquisition procedures to emerging digital technologies in support of Force XXI digitization objectives.

- Coordinating and synchronizing the efforts of combat, materiel, and training developers to develop and deploy Force XXI information technologies.

- Overseeing ATA compliance, to include assuring that system and technical architectures are consistent and that ATA standards are incorporated in contract requirements.

- Maintaining the *ADMP*.

- Coordinating with the Joint Staff and Unified Commands on all *ADMP* matters that impact on interoperability of joint and multinational information exchanges.

- Monitoring Army-wide digitization integration to ensure consistency with the *ADMP*.

- Advising the VCSA and AAE on all matters concerning the integration of digital capabilities across the force.

- Developing and coordinating Memoranda of Agreement (MOA) with the Navy, Marine Corps, and Air Force.

- Coordinating the digitization portion of multinational MOA.

- Coordinating *Red Teaming* of information systems used in Force XXI AWEs to accomplish vulnerability assessments and provide feedback to developers.

- Ensuring that all systems are certified by the Digital Integrated Laboratory (DIL) before providing them to the EXFOR.

2.9 U.S. Army Forces Command (FORSCOM)

FORSCOM is responsible for:

- Providing personnel and resources in accordance with FORSCOM/TRADOC agreements.

- Providing feedback to the ARSTAF concerning the utility of fielded digital equipment.

- Assisting in design and review of joint/multinational information exchange requirements.

2.10 U.S. Army Training and Doctrine Command (TRADOC)

TRADOC is responsible for:

- Redesigning the operating force to be knowledge-based, modular in design, and tailorable in capability.

- Reviewing the annual Total Army Analysis (TAA) and Program Objective Memorandum (POM) for conformance with Army priorities stemming from *Joint Venture* experiments.

- Coordinating *Joint Venture* experiments and findings with other Services and nations.

- Developing and documenting operational requirements associated with the *HIBC MNS.*

- Developing and updating the OA.

- Identifying and tasking appropriate service schools to support the development of the OA by providing Integrated Definition for Function (IDEF) activity models for information systems (i.e., $IDEF_0$); supporting development of system data models (i.e., $IDEF_{IX}$); and developing end-user requirements.

- Planning, programming, and budgeting for: Force XXI training and simulations; Division XXI and Corps XXI experimentation; Applique Force Development Test and Evaluation (FDTE); and any other EXFOR/4ID(M) digitization experiments.

- Designing, planning, resourcing, coordinating, conducting, and analyzing AWEs/BLWEs to provide timely feedback for decisions on Force XXI design.

- Developing training and doctrinal literature for digitization implementation.

- Developing, in conjunction with materiel developers, BLWEs that evaluate and refine the operational capabilities of new equipment and software from the FBCB2 contract, related ATDs, and other digitization-related development efforts.

- Aligning ACT II BLWEs with digitization objectives.

- Providing operational control of the EXFOR Coordination Cell (ECC) at Fort Hood, TX.

- Developing programs in conjunction with FORSCOM, AMC, and PEOs for training EXFOR personnel to operate, employ, and maintain their digital equipment.

- Defining, coordinating, and consolidating joint and multinational information exchange requirements in coordination with the Joint Staff, Unified Commands, DISA and the Joint Interoperability Test Center (JITC).

- Providing appropriate M/S support.

- Developing baseline and modified Tables of Organization and Equipment (TO&Es) to reflect equipment authorizations, new manning levels, and required individual skills emanating from Force XXI digitization efforts.

- Developing criteria for evaluating the operational effectiveness of digitization.

- Reviewing Requests for Proposals (RFPs) and Invitations for Bids (IFBs) to ensure Statements of Work (SOWs) sufficiently address training development and requirements.

2.11 U.S. Army Materiel Command (AMC)

AMC is responsible for:

- Providing matrix engineering support to the Army Technical Architect and PEOs/PMs.

- Serving as the Army's Systems Engineer, reporting to the Army's Technical Architect on technical architecture matters.

- Establishing an Army Systems Engineering Office (ASEO) to support DISC4 in updating the ATA and to provide subject matter experts to Integrated Product Teams (IPTs) preparing SOWs and RFPs.

- Planning, programming, and budgeting for:
  - Maintenance of the ASEO.
  - Development and maintenance of Weapons System Technical Architecture (WSTA).
  - Continued standards development (i.e., MIL STD 188-220A, VMF set, and validation tools).
  - The DIL.
  - The Army Information Network (AIN).
  - Post-Deployment Software Support (PDSS) requirements, to include required changes to embedded system interfaces to comply with the requirement for all systems to migrate to Version 4.0 of the ATA.
  - Army participation in commercial standards bodies.
  - Multinational interoperability efforts.
- Coordinating all information technology generation and application efforts as they relate to the Army digitization effort.
- Developing plans to migrate systems to the ATA, and evaluating the detailed execution plans submitted by PMs, PEOs, and ACTD/ATD managers.
- Interfacing with joint and multinational technical agencies.
- Influencing commercial standards and participating in related fora.
- Providing expertise in assessing the latest information processing technologies.
- Evaluating commercial technologies.
- Establishing and maintaining the DIL to verify interoperability of C3 and Intelligence and Electronic Warfare (IEW) hardware and software.
- Providing appropriate M/S support.
- Serving as the Army executive agent for multinational digitization efforts.
- Coordinating platform integration.
- Ensuring that a system safety program is implemented, associated responsibilities are accomplished, and safety releases are provided IAW AR 385-16 (*System Safety Engineering and Management*).

- Ensuring that PMs execute the Manpower and Personnel Integration (MANPRINT) Program IAW AR 602-2 (*MANPRINT in the System Acquisition Process*).

- Providing technical assistance, subject matter expertise, and materiel support to exercises and experiments.

2.12 U.S. Army Space and Strategic Defense Command (SSDC)

SSDC is responsible for:

- Ensuring that Army programs for the missile defense system developed by the Ballistic Missile Defense Office (BMDO) remain interoperable with evolving information architectures.

- Identifying, evaluating, and coordinating the inclusion of space and missile defense capabilities into Force XXI.

- Providing space and Theater Missile Defense (TMD) M/S support.

2.13 Program Executive Offices (PEO) and Program Managers (PM)

PEOs and PMs are responsible for:

- Providing quarterly digitization reviews.

- Developing plans to migrate to the ATA, including:

  - Integrating FBCB2 software.

  - Providing support to PM Applique to facilitate integration.

  - Developing and documenting necessary program funding and schedule changes.

  - Incorporating digitization test criteria in system TEMPs.

  - Addressing critical digitization initiatives in all program rules.

  - Registering mission applications with the DII through the DII Program Management Office (PMO)

- Certifying compliance with ATA to the Milestone Decision Authority prior to formal release of draft and final RFPs for any experimental or modernization systems that use, generate, or exchange information.

- Providing M/S support for digitization as appropriate.

- Supporting the experimentation process.

- Defining and documenting new potential interfaces with other system platforms through applique or modification to embedded software.

- Accomplishing specified Applique installation kit responsibilities as follows:

  – Responsibilities for tasks associated with the FBCB2 contract and communications systems installation kits will be split between the Applique PM and the various platform PMs/End Item Managers (EIMs). (See Figure 2-1).

  – Installation kits include mounting brackets, holsters, wires, and other similar items. The installation kits do not include line removable applique items.

  – Figure 2-1 depicts which PM has responsibility for each task.

TASK	APPLIQUE PM	PLATFORM PM/ END ITEM MGR
1. Design common installation kit components (e.g., applique mount)	X	
2. Produce installation kits	X	
3. Design platform modifications (e.g., drawings of hole patterns and unique installation kit hardware)	X (Platforms identified in 4/95 contract)	X (Platforms identified after 4/95)
4. Modify platforms		X
5. Install and verify installation kit	X	
6. Verify platform integration		X

Note: ADO is responsible for programming and budgeting for all applique-related tasks.

Figure 2-1 Installation Kit Responsibilities

- Planning, programming, and budgeting for the development and implementation of ATA migration plans.

  – PMs who plan to integrate the FBCB2 software module in their embedded software system are responsible for programming all associated costs including human computer interfaces, safety, system engineering, etc.

  – PMs upgrading embedded system software to incorporate ATA standards are responsible for programming all associated costs.

2.14 PEO for Command, Control, and Communications Systems (PEO C3S)

PEO C3S is responsible for:

- Managing the acquisition and fielding of Force XXI C3 systems.
- Managing the Force XXI system integration effort with support from AMC, to include the development and maintenance of the TF XXI Systems Integration Plan (TSIP).
- Developing software products supporting the COE.
- Evaluating COE candidate products and ensuring that Army COE requirements are provided to DISA.
- Developing, in conjunction with TRADOC, programs to train EXFOR personnel to operate, employ, and maintain their digital equipment.
- Providing appropriate M/S support.
- Creating and updating the Force XXI SA.
- Preparing and overseeing the overarching *Digitization Risk Management Plan.*
- Serving as the ADO's executive agent for the Applique contract.
- Ensuring that all components of the *Tactical Internet* are programmed in the POM.
- Preparing an *Applique EXMP* in coordination with the ADO.
- Preparing, in coordination with the ADO, a capstone *Tactical Internet EXMP.*
- Developing and coordinating all documentation for Milestone Decision Reviews (e.g., the TEMP).

2.15 U.S. Army Operational Test and Evaluation Command (OPTEC)

OPTEC is responsible for:

- Providing an independent evaluation of the operational utility and suitability of digitization hardware and software.
- Planning for and participating in the full series of digitization field experiments.
- Planning, programming, and budgeting for the Applique Initial Operation Test and Evaluation (IOTE), and continued support of EXFOR/4ID(M) experiments
- Providing a continuous and iterative suitability analysis to guide the development process and to support acquisition decisions.
- Serving as the lead evaluation agency supporting the ADO.

- Establishing a rolling baseline to support digitization experiments.
- Providing appropriate M/S support.
- Assisting in development of test plans and procedures for individual AWEs or phased efforts between linked AWEs.
- Reviewing and evaluating training needs and effectiveness.

2.16 Experimental Force (EXFOR): 4th Mechanized Infantry Division

The EXFOR is responsible for:

- Coordinating digitization efforts with the ADO.
- Supporting the experimentation process.
- Providing feedback on the performance and utility of fielded digitized equipment and perceived needs for DTLOMS enhancements.
- Accomplishing applique installation kit responsibilities for tasks listed in Figure 2-1.

3. INTEROPERABILITY FRAMEWORK

In support of the National Military Strategy, the *DII Master Plan* provides an overarching strategy for DoD C4I implementation. Within the DoD framework, the *C4I for the Warrior* concept guides all the Services towards a common, global, C4I warfighting vision.

3.1 C4I For the Warrior

The Joint Staff developed the *C4I for the Warrior* concept as an interoperability objective derived from joint operational requirements. *C4I for the Warrior* envisions a widely distributed user-driven infrastructure in which the warrior plugs–in to obtain information from secure and seamlessly integrated computer and communications systems. Key features of the concept are:

- **Split Base/Reach Back**. The ability of the warfighter and battle staff to deploy and to supplement the warfighters' limited mission support staff with forces in the Continental United States (CONUS) deployed to the forward zone by electronic means.

- **Same Look and Feel.** Systems used by warfighters in garrison and in the field will appear identical.

- **Tailored C4I Information.** The warfighter chooses the types of critical information to be pushed forward to him and has the freedom to pull other needed information when and where it is needed.

All four Services have implemented a framework to overcome the challenges of joint interoperability by synchronizing C4I programs with the *C4I for the Warrior* concept. Each Service's strategy is focused on achieving interoperability through strict adherence to the technical architecture standards established by DoD.

The resulting strategy frameworks are called *The Army Enterprise Strategy* for the Army, *Copernicus...Forward* for the Navy, *Horizon '95* for the Air Force, and *Sea Dragon* for the Marine Corps.

3.2 *Enterprise*

Enterprise synchronizes Army digitization programs with the *C4I for the Warrior* concept, sound business practices, and the *DII Master Plan* while focusing on the information needs of the Army as a whole. It addresses the Army's requirements to organize, train, and equip the digitized force; unique requirements as a component of a joint or multinational force; and the functional requirements for sustaining the force from both a logistical and business perspective.

Enterprise is comprised of the following ten principles:

- **Focus on the Warfighter.** Provide the warfighter with systems meeting validated needs.
- **Ensure Joint Interoperability.** Provide the warfighter with interoperable C4I systems for joint and multinational operations.
- **Capitalize on Space-Based Assets**. Provide the warfighter with assured access to mission-essential military and commercial space-based systems that support the Force Projection Army across the entire operational continuum.
- **Digitize the Battlefield.** Provide the warfighter with an integrated digital information network that supports warfighting systems and assures command and control decision-cycle superiority.
- **Modernize Power Projection Platforms.** Provide the warfighter with a modern power projection platform to support peacetime operations, training, mobilization, force projection, split-base operations, and redeployment.
- **Optimize the Information Technology Environment.** Provide the warfighter with more efficient information support for combat and peacetime operations.
- **Implement Multi-level Security.** Provide the warfighter with the ability to access and exchange information at needed levels of classification using a single C4I system.
- **Ensure Spectrum Supremacy.** Provide the warfighter with electromagnetic spectrum supremacy in order to better visualize the battlespace while blinding or shaping an opposing commander's vision.
- **Acquire Integrated Systems Using Commercial Technology.** Provide the warfighter with synchronized C4I capabilities that leverage commercial technology.
- **Exploit Modeling and Simulation.** Provide the warfighter with cost-effective training, testing, and rapid prototyping through state-of-the-art M/S.

3.3 *Copernicus*

Copernicus and its update, *Copernicus...Forward,* focus on fielding systems that provide rapid access to essential data, allowing the decision-making process to migrate from upper echelons down to the lowest tactical commander. A goal of *Copernicus* is to create the conditions for a true sensor-to-shooter environment.

Emerging Navy and Marine Corps doctrine moves naval operations from the open seas into the constrained littoral regions, requiring a fundamental shift in C4I requirements. Reduced reaction times, combined with increasingly capable land-based threat weapons, makes full integration of C4I and Combat Direction Systems (CDS) a critical objective. *Copernicus* is accomplishing this

integration by prescribing the interfaces between C4I systems and the CDS. These interfaces depend on common standards and protocols for transfer of data between the systems.

The Joint Maritime Command Information System (JMCIS) represents the first major step in fielding *Copernicus.* It links command and control systems into functional categories and creates an environment for all Services to field interoperable systems with common user interfaces. JMCIS forms the first kernel of GCCS.

Five essential elements of *Copernicus* provide architectural oversight to leverage the C4I infrastructure effectively and enhance the operational perspective:

- Tactical C4I information systems connected seamlessly with non-tactical infrastructure.
- Two-way *user pull* and *intelligent push* capability, with the ability to rapidly assimilate information through standardized data formats and condensed data fusion.
- Multimedia (voice/data/video) environment where form fits function.
- Common operating environment to standardize the user-to-computer interface.
- Common building blocks for an expeditious and cost-effective *plug and play* capability.

As an interactive framework of pillars, *Copernicus* links the command and control processes of the warfighter at all echelons of command. The pillars of *Copernicus* include:

- The Global Information Exchange System (GLOBIXS), which supports joint and multinational tactical commanders by providing access to required information from any location through a series of wide area Defense Communications System (DCS) networks.
- The Commander–in–Chief (CINC) Command Complex (CCC), which serves as the primary gateway for communications and information flow from GLOBIXS to forward deployed warfighters. The CCC performs command and control, correlation, and fusion functions. A commander's decision-making capability with a focus on rules of engagement and operational intent is included. Battlespace decisions are made by the tactical commanders and their shooters.
- The Tactical Data Information Exchange Systems (TADIXS), which are the tactical networks connecting the CCCs with the Tactical Command Centers (TCCs). These tactical networks fall into four general categories: command, direct targeting, force operations, and support. TADIXS provide enhanced digital communications links to the shooters' combat systems within the *Copernicus* infrastructure, enabling user-pull functionality and enough computer power and bandwidth to receive and process tactical information.
- The TCC, which disseminates information to the warfighter. The TCC can be any forward deployed command center—ashore or afloat, mobile or fixed—and includes tactical

centers for individual units. Employing Tactical Digital Information Links (TADILs), TCC is the gateway for information flow between TADIXS, the shooter, and the weapons.

- The Battlecube Information Exchange System (BCIXS), which extends the architecture to include the battlecube, the area in which shooters and weapons reside. The battlecube is a conceptual, multi-dimensional area that includes subsurface, surface, air, and space as the environment for conducting warfare, similar to the joint concept of battlespace. BCIXS represents the battlecube in which tactical forces operate, with fluid boundaries defined by the dynamics of the battle. Shooters operating in the battlecube form the operational nodes in the BCIXS.

3.4 *Horizon*

The first version of *Horizon* focused on Air Force information architectures by advancing the premise of an integrated and responsive global infosphere supporting Air Force *Global Reach, Global Power* objectives. The second version expands on the original concept by establishing an Air Force vision for 21st Century C4I infrastructure and for enabling the integration of information technology. Included in *Horizon* is the *Communications Squadron 2000* initiative, which redesigns the C4 force structure for deployed wings and base support infrastructure. The C4 capabilities deployed with combat wings will plug into joint networks in the theater, accessing the infosphere and providing commanders with real-time information on demand.

The *Horizon* vision will be achieved through compliance with a standards-based information architecture, rapid assimilation of technology, common sense plans and policies, forward-looking vision, and sound resource management.

Horizon envisions the warrior exercising command and control using a user-transparent common operating environment of distributed, collaborative planning, and smart push-pull information facilities. Knowledge-based C4I systems will foster the ability to *push* designated information to the user while simultaneously permitting the user to *pull* additional information from the digital environment as needed.

Horizon recognizes the information realm as a new mission area. To achieve superiority in this new dimension, commitment is required by all echelons of command to field new technologies, provide training, and develop the required support structure. Technology advances, shrinking defense budgets, and force reductions dictate the need to incorporate high leverage information technology into every aspect of military operations.

3.5 Sea Dragon

Sea Dragon is a futuristic concept for a smaller, more lethal Marine Corps of the 21st Century. The Corps will remain closely allied with the Navy, with primary mission focus on littoral operations and enabling missions as an early-deploying component of a joint task force. The 21st Century Corps will operate at a greater width and depth on the battlefield, maximizing the use of supporting arms to disrupt and destroy the enemy. Small independent units with improved targeting and C2 will apply firepower-based tactics employing indirect fires and air-to-ground

delivery systems, rather than traditional *close-with-and-destroy* maneuver-based tactics. *Sea Dragon* will be heavily reliant on sea-basing of fire support, logistics, and C2 assets.

The future Fleet Marine Force (FMF) will retain a semblance of the current structure with an Air Combat Element (ACE), a Ground Combat Element (GCE), a Combat Service Support Element (CSSE), and a Command Element (CE). However, the FMF will be smaller, lighter, more mobile, and more versatile. In the *Sea Dragon* FMF:

- Emphasis will be placed on the use of unmanned vehicles for logistics, medical evacuation, and close air support. Close-in fire will be provided by unmanned aerial vehicles (UAVs) operated by the GCE. Manned aircraft will be utilized for deep strike missions, with the ACE operating primarily from ships. The MV-22—able to travel farther and faster than its predecessors—will significantly alter heliborne operational doctrine.

- The GCE will transition to a lighter force that is organized, trained and equipped to conduct small, independent operations. A Marine division will be composed of two light (infantry) regiments, one heavy (mechanized) regiment, and an up-gunned artillery regiment. The heavy regiment will conduct conventional assaults, defenses and counterattacks. The light regiments will be organized around restructured infantry battalions of 400-500 Marines.

- Rapid assault squads (RAS) drawn from the light battalions will operate independently in their assigned *zones of action* to gather intelligence and to seek out enemy formations and positions. Once pinpointed, the RAS will continuously engage them with aerial and indirect fire weaponry, creating confusion and presenting the enemy commander a multitude of events to deconflict. The RAS will be equipped with the latest target designating and locating devices and will be linked into a C2 system providing rapid access to supporting arms and control agencies.

- The CSSE will be structured to operate from shipboard with no more than a limited footprint ashore. CSS will be integrated into the C2 system in order to anticipate demand for supplies and services through an automated process.

- The CE will be structured to conduct most activities from aboard ship, with the C2 system providing a common battlefield picture.

The *Sea Dragon* concept places maximum emphasis on intelligent and highly educated Marines, improved simulation-based training, and integrated battlefield application of modern technology. Current plans call for deploying an operational *Sea Dragon* Marine Expeditionary Unit (MEU) in early 1998.

THIS PAGE INTENTIONALLY LEFT BLANK

4. ARCHITECTURE

4.1 DoD Architecture Initiatives

There are several DoD initiatives that have a direct impact on the architectures being developed for Army digitization and on the *ADMP*.

4.1.1 Technical Architecture Framework for Information Management (TAFIM)

The Technical Reference Model (TRM) for Information Management was the initial effort to bring commonality and standardization to DoD's technical infrastructure. Although the TRM addressed the services and standards required to implement a common technical infrastructure, a single TA framework was still needed to integrate these efforts and drive systems design, acquisition, and software re–use throughout DoD.

TAFIM was developed to meet that requirement. It provides the DoD-wide framework to manage multiple TA initiatives and is intended to achieve the following results:

- Use of common principles, assumptions, and terminology in DoD TAs.
- Definition of a single structure for DoD technical infrastructure components and how they are managed.
- Development of information systems in accordance with common principles to permit DoD-wide integration and interoperability.

TAFIM does not provide a specific architecture. It provides the services, standards, design concepts, components and configurations used to guide development of TAs meeting specific mission requirements. TAFIM is independent of mission-specific applications and their associated data. System architects and designers will use TAFIM as the basis for developing a common target architecture to which systems can migrate, evolve, and interoperate.

Proper application of the TAFIM guidance will:

- Promote integration, interoperability, modularity, and flexibility.
- Guide acquisition and re–use.
- Speed delivery of information technology and lower its costs.

TAFIM introduces and promotes *interoperability*, *portability*, and *scalability* of DoD information systems. Over time, the number of compliant systems will increase, providing users with improved *interoperability* needed to achieve common functional objectives. To achieve *portability*, standard

interfaces will be developed and implemented. *Scalability* will be developed in mission applications to accommodate functional flexibility.

4.1.2 DoD Open Systems Policy

4.1.2.1 Open Systems Standards

In a policy memorandum dated 29 June 1994, the Secretary of Defense stated his commitment to "a new way of doing business" in DoD, to include the use of open systems (consensus-based, public, or non-proprietary) specifications and standards. To this end, his memorandum directed that the preference for use of specifications and standards within DoD systems acquisitions be performance, commercial, and military, in that order. It further stated that requests to use other than open systems standards would require a waiver.

Based on that policy guidance, the ATA is heavily oriented toward the use of open systems standards. For example, the architecture for the Army *Tactical Internet*—the key communications component of the Army's Force XXI initiative—is based on the architecture and open system standards being used by the world-wide Internet.

4.1.2.2 Open Systems Joint Task Force

In a subsequent memorandum dated 29 November 1994, the Undersecretary of Defense for Acquisition and Technology directed that open systems specifications and standards be used for acquisition of weapons systems electronics to the greatest extent practical. He established a joint oversight office—the Open Systems Joint Task Force (OS-JTF)—to ensure implementation of this policy. As amplified in the *OS-JTF Charter*, the focus of this group is on the acquisition of new systems and system upgrades to electronics embedded in weapons systems and platforms. It is not oriented on C3I systems, communications networks, or real-time data processing functions.

Previous versions of the ATA focused mainly on systems and communications networks used to support C3I activities in the tactical environment. In response to the Undersecretary's guidance, the Army is addressing embedded electronics in the most recent version of the ATA (see Section 4.2.2.1.5, Planned Enhancements to the Technical Architecture).

4.1.3 Common Operating Environment (COE)

4.1.3.1 Global Command and Control System (GCCS)

GCCS has been designated the single command and control system for DoD. GCCS improves the joint warfighter's ability to manage and execute crisis and contingency operations. It provides a means to interface with joint, Service-specific, and Federal agency C4I systems for peacetime deliberate planning, as well as crisis planning and execution. (see section 5.1, Army GCCS)

The need for GCCS stems from lessons learned from previous conflicts, current/projected operational requirements, and the effects of rapidly changing technology. The warfighter requires a seamless information system, in which boundaries between functions and sources are erased.

GCCS provides seamless, integrated information to the warfighter when, where, and how it is needed. The goals of GCCS are:

- To provide one affordable system that integrates across Services and functions to provide the warfighter with a single picture of the battlespace.

- To migrate legacy applications to modern computing principles and technologies through the use of a COE.

The COE is an outgrowth of the GCCS effort to achieve the latter goal.

4.1.3.2 COE Development

The development of the current DII COE stems from the GCCS COE effort, and is perhaps the most significant and useful technical by-product of the GCCS development effort. The initial impetus behind GCCS was the replacement of the World Wide Military Command and Control System (WWMCCS), with additional goals of improving C2 interoperability and reducing duplicative C2 system developments. Services and agencies nominated products for incorporation into a COE focused on supporting the WWMCCS replacement. A number were used to create the initial versions of the COE, with the remaining products to be incorporated into later versions of the COE as it expanded to support other systems.

As an outgrowth of this effort, the Services and agencies have agreed to migrate their C2 systems to the DII COE, having independently arrived at similar conclusions. The COE is in reality very simple and straightforward, but powerful in its ability to tailor a system to meet individual site and operator requirements, while retaining the architectural freedom to evolve.

4.1.3.2.1 Fundamental COE Concepts

In COE-based systems, all infrastructure and mission application software—except the operating system and basic windowing software—is packaged in self-contained units called *segments*. Segments are the most basic building blocks from which a COE-based system can be built and are defined in terms of the functionality they provide. The principles which govern how segments are loaded, removed, or interact with one another are the same for all segments, but *COE component segments*—which are part of the COE—are treated more strictly because they are the foundation on which the entire system rests. Only the segments required to meet a specific mission application need to be present, allowing a minimization of hardware and software resources required to support a COE-based system.

The terms *interoperability* and *integration* are tightly defined in the context of the DII COE. Interoperability refers to the ability for two systems to exchange data unambiguously; with no loss of precision; in a format understood by both systems; and in such a way that interpretation of the identical data is precisely the same. Integration refers to combining segments—not systems—and ensuring that the segments work correctly within the COE environment; do not adversely impact one another; and conform to COE standards. Integration does not imply interoperability. It only provides a level of assurance that the system will work as designed.

4.1.3.2.2 DII COE Integration and Runtime Specification (I&RTS)

The latest I&RTS, dated 23 October 1995, divides the COE into a series of segments, with agencies assigned responsibility for each. Figure 4-1 depicts this schematic, while also identifying the *kernel* COE components, which are the minimal set of software required on every COE workstation.

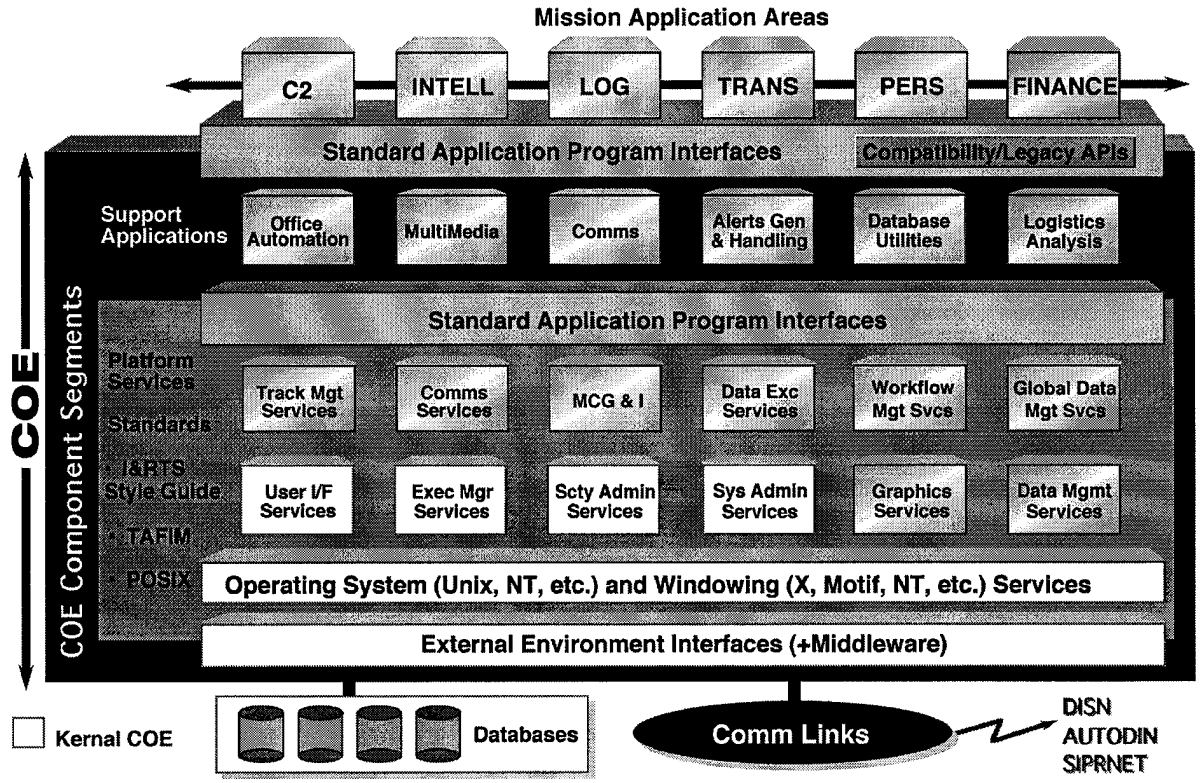


Figure 4-1 Defense Information Infrastructure Common Operating Environment (DII COE)

The DII COE I&RTS provides substantive COE guidance to PMs and developers, while also providing DISA with a means to check COE compliance. It includes the process of registering a mission application with the DII PMO, how to segment mission applications for interoperability with other DII-approved applications, and how to manage the DII environment. As a first step to *C4I for the Warrior* (*C4IFTW*) and COE compliance, PMs should register their mission applications with GCCS. DISA will issue the developer a unique root directory name under the overall GCCS directory structure. This will guarantee *C4IFTW*-type capability in that any mission application can be loaded on any authorized GCCS device worldwide. The next step is segmenting and testing the software to ensure peaceful coexistence with all other GCCS-registered mission applications. This entire process is described in the DII COE I&RTS, which is accessible via the World Wide Web at http://164.117.208.50.

4.1.3.3 COE Compliance

The current Defense Planning Guidance for FY1997 to FY2001 mandates the use of the COE as the target system for all DoD systems. The COE is an integral part of the ATA, and the AAE has mandated that implementation plans for compliance with the ATA and migration to the COE must be submitted for all systems.

At present, the GCCS COE is mandated by the ATA. However, GCCS is transitioning to the broader umbrella of the DII, and the Army is committed to mandating the DII COE and its associated Applications Programming Interfaces (APIs) as they evolve. Version 1.0 of the DII COE was released in February 1996, and the DII COE System Engineer has indicated that mission application developers should now be targeting migration of applications to the DII COE instead of the GCCS COE. As such, the Army intends to focus on DII COE compliance, and plans to use the specific criteria provided in DII COE I&RTS Section 2.1.3 for evaluating compliance.

4.1.4 Other Architecture-Related Initiatives

Although not architecture initiatives by definition, there are a number of recently promulgated DoD policies that have a significant impact on Service/agency architectures. The most noteworthy are the policies associated with the Defense Message System, Tactical Data Link Standard, and Data Element Standardization.

4.1.4.1 Defense Message System (DMS)

In a series of policy memoranda, the Assistant Secretary of Defense for C3I (ASD(C3I)) stated that DMS would be the single messaging system for all DoD fixed, mobile, strategic, and tactical environments. The policy dictates that all DoD electronic messaging (i.e., AUTODIN and legacy electronic mail) must migrate to DMS-compliant messaging as rapidly as possible.

Architecturally, DMS is based on the International Telecommunications Union (ITU) X.400 series of recommendations, with extensions to meet U.S. security requirements. Because of these security requirements, a directory service based on the ITU X.500 series of recommendations is required for DMS operation. However, the X.500 directory service has architectural implications that extend beyond mail and messaging to encompass other functions, such as security and file transfer services.

The Army has incorporated DMS-compliant X.400 and X.500 standards into its ATA. An *Army DMS Transition Plan* has been submitted to DISA's DMS PMO showing how and when DMS components and services will be phased into the Army. Planning is underway for necessary changes to organizations, procedures, and training, and for the acquisition and/or modification of equipment required to implement the plan. AUTODIN replacement is the Army's first priority.

In the first implementation phase, the Army plans to provide DMS messaging and electronic mail capability to all current strategic and tactical AUTODIN users down to maneuver brigade level. In succeeding phases, additional users (e.g., current e–mail users without AUTODIN access) will be provided with a DMS capability.

4.1.4.2 Tactical Data Link Standard

In October 1994, ASD(C3I) published a policy memorandum designating Link 16 as the DoD primary data link for processed information for C2I applications and—where practical—weapons systems, unless an exception is granted by ASD(C3I).

A Joint Tactical Data Link Working Group (TDLWG) was established to prepare a management plan and listing of data links or systems covered by the policy, along with a coordinated migration plan and legacy data link support strategy. For the purposes of the management and migration plans, the TDLWG agreed that Link 16 is the J-Series Family, consisting of F-series (i.e., North Atlantic Treaty Organization (NATO) Link 22), J-Series (i.e., Joint Tactical Information Distribution System (JTIDS)), and K-Series (i.e., VMF), together with the related information transfer standards (e.g., Military Standard (MIL-STD) 188-220A for VMF).

VMF messages intended for use on the Army *Tactical Internet* were derived from the TADIL J/Link 16 and other jointly agreed data elements. However, addressing and naming conventions are very different and user-transparent gateways and/or dual language hosts will be needed to allow interoperability. The Army will ensure that Link 16 messages and data elements are used to the maximum extent possible, and will work with DoD and the other Services toward an architectural goal of consolidating Link 16 and Army/Joint VMF messaging at some future date. Section 4.2.2.1.3 (Information Modeling and Data Exchange Standards) provides additional information.

4.1.4.3 Data Element Standardization

The ASD(C3I) data element standardization policy states that the Defense Data Dictionary System (DDDS) is the DoD-wide integration point for standard data element definitions. This policy requires the Services, agencies, and unified commands to document the data elements used by their automation processes and to submit them to the DDDS for standardization.

In compliance, the Army has incorporated two IDEF method models into its ATA ($IDEF_0$ process model and $IDEF_{1X}$ data model). This provides both technical guidance and the mechanism by which developers can document data and submit the associated data elements to the DDDS for standardization. See Section 4.2.2.1.3 (Information Modeling and Data Exchange Standards).

4.2 Army Architecture Strategy

To achieve the vision and goals of Force XXI, all battle command systems must be flexible and interoperable. The battle command information infrastructure must support the ability to structure a force rapidly and efficiently to meet any future contingency. Given the split-based operations requirements of a force projection Army, interoperability and flexibility are necessary between tactical systems and the post, camp, and station information systems. Moreover, the need for interoperability and connectivity of battle command systems is not just an intra-Army issue. The need to conduct joint and multinational operations requires open, flexible, and interoperable information infrastructures and the ability to facilitate STOW training.

In 1994, the Army Science Board (ASB) presented the results of its study on a technical (information) architecture for C4I systems. In its final report, the ASB defined technical architecture, differentiated it from operational and system architectures, and recommended a process and organizational structure for developing and enforcing an Army-wide technical architecture. The Army has implemented the ASB's recommendations.

4.2.1 Operational Architecture (OA)

An operational architecture is a description—often graphical—which defines the *force elements* and the requirement to exchange information between these force elements. It defines the types of information, the frequency of information exchange, and which warfighting tasks are supported by these exchanges. It also specifies what the information systems are operationally required to do and where these operations are to be performed.

The Force XXI OA is being developed by the TRADOC Combined Arms Center, with technical support from PEO C3S. It will provide a detailed breakout of functions, processes, and information flows, and will be developed over an extended period of time in an evolutionary process. In the near–term, the OA for TF XXI will serve as a proof–of–principle for expanded, follow-on versions. It is being developed in two phases:

- Phase I: focused on brigade-and-below mounted maneuver, with limited Combat Support/Combat Service Support (CS/CSS) functions.

- Phase II: will continue as a proof-of-concept to serve as a baseline for follow-on operational architectures. Focus will remain on the Task Force XXI (brigade-and-below) operational elements, with emphasis placed on those functions as jointly determined by the operational and system architects. Priority of effort will be to command, primary staffs, fire support, air defense, and forward support battalion functions. Phase II is scheduled for completion in June 1996.

Development and analysis of the OA will use modeling tools, logical connectivity diagrams, value–added methodologies, assessments of battlefield return–on–investment, and database development.

- Modeling will follow TA-mandated IDEF techniques and be compliant with Federal Information Processing Standards (FIPS) Publications 183 and 184. IDEF modeling will be executed under $IDEF_0$ (activity/functional) modeling and $IDEF_{1X}$ (data) modeling, employing a fully attributed model mapped to the C2 Core Data Model.

- Connectivity analysis and diagrams will show required connectivity among and between TF XXI operational elements and display the types of information to be passed. Analysis will incorporate the use of table-top analytical methods, military judgment, subject-matter experts, and IDEF modeling results.

- Since IDEF models do not incorporate executable databases, analytical results from the modeling effort will be captured in a relational database along with all performance

parameters (e.g., information flow requirements among and between operational elements, information content, frequency of transmission, speed of service, perishability, cost of failure, and security classification level). This singular, multi-compatible database can be used for dynamic depiction of architecture structures and identification of requirements, capabilities, and effectiveness. The relational database can also provide support for other M/S efforts and requirements documents updates.

Development of operational architectures for the Army will be executed in a *spiral development process*. The start point is TF XXI, with multi-echelon brigade and division development now occurring simultaneously. New operational architectures will be developed as proposed force structures for Force XXI are constructed, modeled, and evaluated.

4.2.2 Technical Architecture (TA)

A technical architecture is the minimal set of rules governing the arrangement, interaction, and interdependence of parts or elements that together may be used to form an information system.

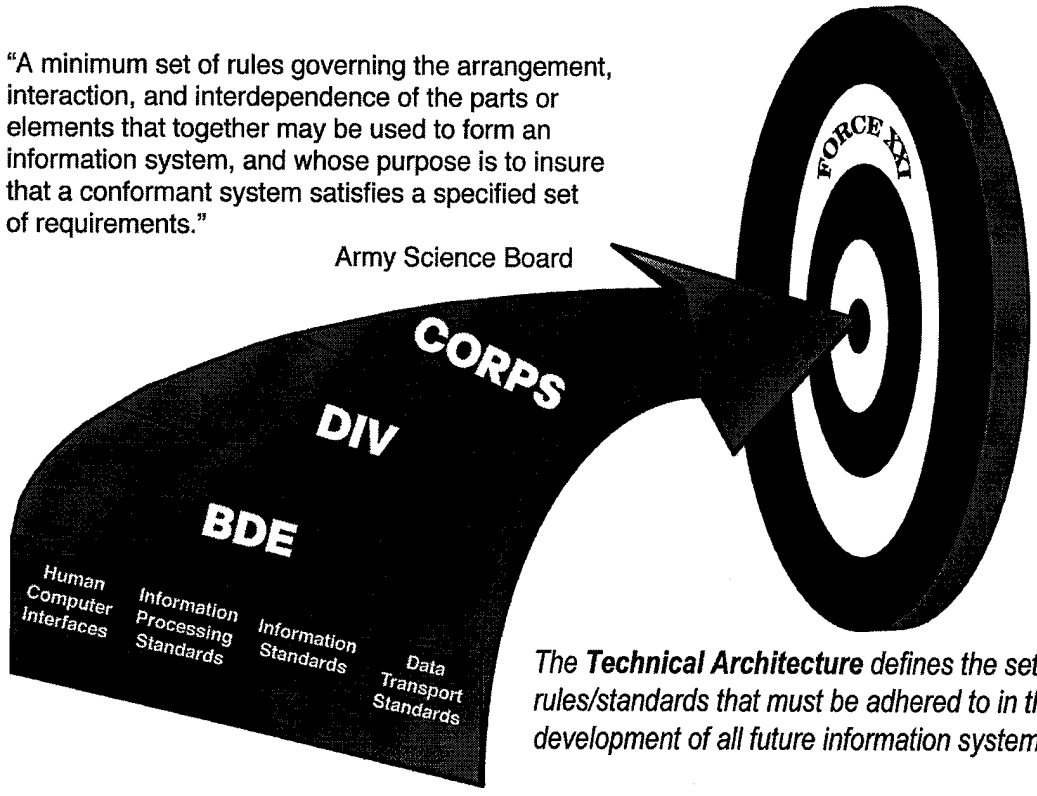


Figure 4-2 Technical Architecture

Its purpose is to ensure that a conformant system satisfies a specified set of requirements. It is the building code for the system architecture being constructed to satisfy operational architecture requirements. Standards laid out in a technical architecture establish the framework for achieving interoperability and commonality among component hardware/software and attaining seamless connectivity between communications systems operating in a digital battlespace.

4.2.2.1 Army Technical Architecture (ATA)

The ATA is an open systems architecture that is compliant with DoD standards and makes maximum use of commercial standards, consistent with mission requirements. Where commercial standards prove inadequate, efforts have been initiated to incorporate required military features into the system and—if possible—into the commercial standards. The architecture was developed in collaboration with the ARSTAF, ASB, ASEO, MACOMs, and PEOs/PMs, based on two primary sources:

- Widely accepted commercial standards for information processing and transport.
- Guidance provided in the DoD TAFIM.

ATA Version 4.0 was approved by the VCSA and AAE on 30 January 1996. Each Army Milestone Decision Authority (MDA), MACOM, PEO, PM, ATD Manager, and ACTD Manager is responsible for ATA compliance for all Army systems that electronically produce, use, or exchange information. Specific migration schedules will be integrated with programmed system upgrade windows.

The ATA groups Army systems into the following categories or *domains*:

- **C3I**. Previous versions of the ATA were focused primarily on standards for the C2, communications, and IEW systems which comprise this domain.
- **Weapons System**. A WSTA Working Group (WG) was formed in May 1995 as the first step in expanding the scope of the ATA to focus more closely on these systems. This WG has developed a course of action which includes scope, technical approach, responsibilities, timelines, milestones, and required resources. Weapons system-associated ATA exceptions and/or extensions are documented in the ATA as they are developed and approved. These exceptions/extensions will maintain interoperability as currently defined in the ATA, while extending the ATA into areas such as hardware, power management, diagnostics, and software re–use standards.
- **Sustaining Base/Office Automation**. This domain consists of automated systems that provide service support, business, and office automation functions. The widening proliferation of these types of systems in the battlefield support role, in parallel with the development of the *reachback* concept, has caused the conformance of these systems to the ATA to become increasingly important. Correspondingly, the scope of the ATA has been expanded to focus more heavily on standards for these systems.

- **Modeling and Simulation**. This domain contains standards that support architectural efforts to combine live, virtual, and constructive modeling and simulation for training and combat analyses.

ATA Version 4.0 addresses five major topics:

- Information processing standards.
- Information transport standards.
- Information modeling and data exchange standards.
- Human–computer interfaces (HCI).
- Information security standards.

The ATA takes advantage of commercial investment in information technologies. It will not remain static, but will evolve through participation with DoD, industry, and international standards organizations in order to identify emerging trends and standards.

4.2.2.1.1 Information Processing Standards

Within the ATA, information processing standards identify a suite of commercial and government standards and associated implementation profiles that are consistent with the TAFIM TRM and standards profile. Compliance with a standard information processing profile promotes development of integrated applications that share functions and data.

As discussed in 4.1.3.2, a COE is the set of integrated support services supporting mission application software requirements. It also provides a corresponding software development environment, architecture principles, and methodologies which assist in the development of mission application software by capitalizing on infrastructure support services.

The Army is committed to using the DII COE. Where necessary, the Army will extend the COE to fulfill specific support requirements for battlespace command and control systems, and will provide those COE extensions to other Services and the DII PMO.

One of the fundamental concepts of the COE is that shared services will be available to other mission applications through standard APIs (See Figure 4-1). These shared services comprise the COE. Interfaces will be designed and documented so they are easy for developers to understand and use. APIs will be baselined and changed only when with the agreement of the affected parties, using a formal configuration management procedure.

4.2.2.1.2 Information Transport Standards

Within the ATA, information transport standards define the communications support required to provide seamless, reliable, and timely information exchange between users. Communications systems and related network interfaces define the topology of the system, and common protocols provide the means necessary for seamless information exchange between users.

Within the ATA, information transport standards are primarily focused on protocols and profiles for packet data exchange. They are grouped as follows:

- **Host Standards** which apply to the transfer of information after a network has been established (end-to-end, user-to-user transfer) involving more-capable processing elements (hosts, workstations, servers, etc.), e.g., the File Transfer Protocol (FTP), Transmission Control Protocol (TCP), and Internet Protocol (IP) standards.

- **Router Standards** which apply to the exchange of connectivity information between routers, e.g., the Border Gateway Protocol (BGP) standard.

- **Network Standards** which apply to the accessing of communications links and networks that will support Force XXI (e.g., the Point-to-Point Protocol (PPP), Ethernet, X.25, and MIL-STD 188-220A standards).

The common thread in Army digital data communications will be use of the Internet protocol suite (e.g., TCP/User Datagram Protocol (TCP/UDP) and IP). In Army data communications networks, unique protocols will continue to exist due to military-unique communications requirements. Most notable is MIL-STD 188-220A, a suite of protocols used with Combat Net Radio (CNR) systems, such as SINCGARS.

4.2.2.1.3 Information Modeling and Data Exchange Standards

Within the ATA, information modeling and data exchange standards pertain to process models, data models, data definitions, and data exchanges. They provide the basis for information-sharing across boundaries. Without such standards, it would be necessary to build and maintain individual interfaces, a costly alternative often resulting in inconsistent and unreliable data from multiple sources.

The ATA mandates a model-based approach to data standardization which consists of:

- **IDEF$_0$**. An activity model that shows the relationship between an activity and the information that it uses or produces. IDEF$_0$ provides standardized procedures and diagramming conventions consisting of:

  - *Node trees* which graphically portray hierarchical activities.

  - *Context diagrams* which show the highest level activity and its inputs, controls, outputs, and mechanisms.

- *Decomposition diagrams* which depict lower-level activities and their information relationships.

Documenting requirements from Operational Requirements Analyses (ORAs) and associated User Functional Descriptions (UFDs) in the $IDEF_0$ conventions will provide a common way to depict the processes and Information Exchange Requirements (IERs) within and between functional areas. Efforts have been initiated to depict the information flows identified in the brigade-and-below ORA in $IDEF_0$ conventions.

- **$IDEF_{1X}$.** A data model which builds on the activity model. $IDEF_{1X}$, a methodology created to help design data, provides a structured notation and syntax consisting of:

  - A set of diagrams containing entities, their attributes, and their relationships.

  - A glossary which defines the entities and attributes.

  - Business statements, which are detailed, written descriptions of the way in which data relate to other data.

  The C2 Core Data Model uses $IDEF_{1X}$ notation and modeling conventions to describe the core data required across all C2 sub-functional areas and presents a common approach to describing tactical C2 information. It consists of 165 entities and more than 800 attributes. These attributes, together with their definitions and associated metadata (data describing data elements), will form the basis for submission of candidate standard data elements to the DoD data standardization program. The C2 Core Data Model is the foundation for the development of standard data elements and will be extended as necessary to reflect data requirements specific to battlespace digitization.

- **Standard Data Elements.** Technical, procedural, and methodological conventions used to establish standard data elements, including metadata and modeling products as documented in DoD 8320.1 series guidance (*Standard Data Elements for Automated Information Systems Design and Development*).

- **Data Dictionary.** Data dictionary or other repository for standard data elements.

Historically, lower-echelon information systems have been primarily messaging and display systems. As evolving systems incorporate database capabilities and require seamless interoperability with information systems at brigade-and-above, there is a pressing need for data standardization across the varied battlespace information systems and operational message sets. Efforts to standardize messages and data elements must be integrated using standard data elements defined in the C2 Core Data Model, which will be extended as needed to accommodate additional data elements and relationships. A far-term goal is to eliminate the need for message sets, such as the character-oriented Joint Interoperability Command and Control System (JINTACCS) U.S. Message Text Format (USMTF), and execute direct database-to-database transfers. Except for the sustainment of multinational gateways, elimination of character-oriented message sets is anticipated to occur around the 2005 time frame.

Technical Interface Design Plans (TIDP) provide a common standard for formatting bit-oriented messages. The TIDP for TF XXI has identified a set of VMF messages oriented on the digitization requirements outlined in the ORA for brigade-and-below. To satisfy operational requirements, IERs are being translated into VMF messages by leveraging existing/common data elements. As a result of future lessons learned during the digitization process, it may be necessary to add to or modify the current VMF message set to better support evolving operational requirements.

Other information standards included in the ATA address imagery (e.g., National Imagery Transmission Format Standard (NITFS)), graphics (e.g., Computer Graphics Metafile (CGM)), and symbology (e.g., MIL-STD 2525).

4.2.2.1.4 Human–Computer Interfaces (HCI)

Standardizing HCIs across application software to attain a user interface that presents a common appearance and behavior among Army systems within the digital battlespace requires a common set of HCI standards and a common approach to implementing them. The Army is developing guidance that will accomplish this, to be contained in documents called *style guides.*

Volume eight of the DoD TAFIM contains the *DoD HCI Style Guide*, which sets the basic graphical HCI standards for Army systems. However, the *DoD Style Guide* is a general document that outlines the basic display standardization needs of the larger DoD community. It does not achieve the level of detail needed for interoperable tactical support systems that exhibit a common look and feel.

User interface specifications for GCCS define the user interface for GCCS applications. This style guide is focused on the information management and X-Windows environment of the GCCS community and supplements the basic guidelines in the DoD style guide to assure that GCCS applications display a common look and feel across the GCCS platforms. The *GCCS Style Guide* is TAFIM-compliant and references the *DoD Style Guide*.

DoD HCI and GCCS user interface specifications establish the basic interface standards for Army command and control system developers. However, in both of these style guides, the primary method of user interaction is through a graphical user interface (GUI) with provisions for an alternative mode of interaction using a character user interface (CUI). Applications that present graphical displays—such as maps—are accessible only through a GUI, while applications that present non-graphical information—such as text or tables—can be accessed through either a GUI or CUI. The benefit of a CUI is that it requires far less transmission bandwidth. Since the bandwidth available to many battlespace users is very constrained, a CUI is necessary to provide them with access to their essential applications.

HCIs will be addressed as MANPRINT issues in specific BFA applications to insure that software /style guides are suitable for the echelon and application for which the software is written.

4.2.2.1.5 Information Security

Security requirements and engineering should be addressed in the initial phases of design. OA decisions regarding the security services to be used and the strength of the mechanisms providing the services are primary aspects of developing the distinct security architectures to support specific domains, using the information security standards in the ATA. They can also be used to assess the relevance of standards that can be met with government-provided components and protocols by using the ATA as a tool to judge the elements of the SA against operational security requirements, standards compliance, interoperability, and reduced costs through re–use.

4.2.2.2 Planned Enhancements to the ATA

Planned enhancements are intended to:

- Incorporate improvements based on feedback from Version 4.0 and ongoing work by the WSTA WG.
- Continue the process of replacing DoD and MIL-STDs with equivalent open commercial standards, where feasible.
- Update referenced standards and profiles to the current approved version.
- Move *emerging* standards to *mandated* standards when they have sufficiently matured.
- Reflect changes in foundation documents such as the TAFIM.
- Resolve issues arising from use of the ATA as the baseline document for a Joint TA.

4.2.2.3 ATA Migration Strategy

The Army strategy for migrating systems to compliance with the ATA is as follows:

- New systems shall comply with the ATA.
- Planned upgrades to existing systems shall comply with the ATA.
- Where cost, schedule, and performance constraints permit, existing systems shall migrate to compliance with the ATA.

All RFPs for new systems or significant upgrades to existing systems will be reviewed for compliance with the ATA. The ASEO serves as a member of the IPT established to review proposed RFPs or Broad Agency Announcements (BAAs) for experimental and modernization systems; reviews the RFP for compliance; and coordinates with the ADO and DISC4. The IPT and the appropriate PEO or MACOM jointly certify compliance to the MDA prior to RFP release. (See Figure 4-3).

The AAE has directed that PEOs/PMs, ATD/ACTD Managers, and MACOMs prepare and submit plans for migrating their systems to full compliance with the ATA. Each plan, consisting of a proposed implementation plan and identification of cost, performance and schedule impacts, is submitted to the ADO. The ASEO reviews these plans to determine compliance with the ATA and provides its evaluations to the ADO.

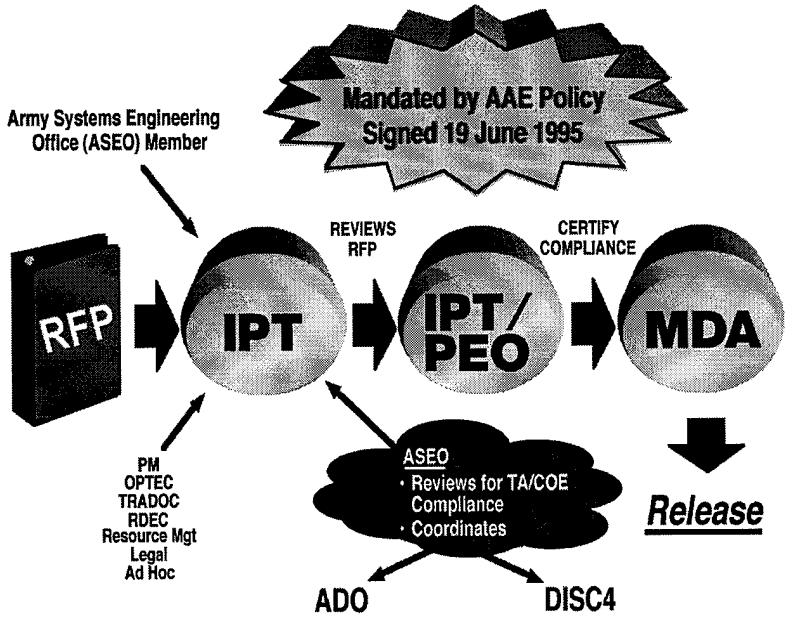


Figure 4-3 Army Digitization RFP Review Process

The first stage of the ASEO review was completed in July 1995 and addressed completeness of the initial submissions. It resulted in several requests for clarification and/or additional information. The second stage entails a technical review covering methodology, cost/schedule impacts, and acceptability.

A number of systems have already initiated ATA compliance efforts in terms of adherence to applicable guidelines, specifications, standards and documentation. For example:

- PEO C3S has developed plans to assure migration of AGCCS, ATCCS, and FBCB2 to COE compliance. Working jointly with DISA, PEO C3S will develop COE *build tapes* that will be provided to PMs. PMs will segment their software and—at a minimum—port the software to the COE kernel while integrating their applications with the COE libraries, consistent with their individual transition plans. The transition started in 1995, and is expected to be completed no later than 2000.

- PEO ASM has incorporated ATA-compliant components in designs for the next generation M1A2 Abrams System Enhancement Program (SEP) and M2A3 Bradley. The M1A2 SEP design re–uses FBCB2 software, hosted on a dedicated C2 processor. The M2A3 plan is to develop interim C2 with a planned migration to FBCB2 software upon completion of the Limited User Test (LUT) scheduled for November 1997.

It is the intent of the ADO to foster a policy of forward compatibility when technically feasible and affordable. Existing systems will migrate to ATA-compliant protocols, profiles, data elements, and message standards. However, when neither feasible nor affordable, interim measures such as translating gateways will be used to provide interoperability between legacy and ATA-compliant systems. Such interim measures must be formally approved by the ADO.

4.2.2.4 Applicability to Joint Operations

Individual digitization efforts of the four Services impact on each other due to the need for digital interoperability in a joint environment. To facilitate joint interoperability, the ATA is based on the use of existing commercial or military standards where possible. However, in those instances where new standards must be developed or existing standards must be modified, the Army's approach is to submit applicable standards for joint approval and adoption.

Standards for data communications via CNR are specific examples of both new and modified standards which have joint applicability. Five CNR standards were submitted for DoD joint standardization review. The two most notable are:

- MIL-STD 188-220A, which is structured in accordance with the Open System Interconnection (OSI) Reference Model, contains a suite of network access protocols used for data communications via CNR-based networks. This standard, along with three others associated with VMF messaging in the tactical environment, was formally approved for joint use on 27 July 1995.

- The VMF TIDP, which provides standards for the format and content of 51 bit-oriented messages used for the real-time or near real-time exchange of data between tactical users. Messages in the VMF TIDP were derived from messages contained in the DoD Link 16 standard. The Army expects approval of its VMF TIDP message submittal by the Joint Configuration Control Board o/a May 1996.

The ATA was selected to serve as the Joint Technical Architecture baseline by ASD(C3I) on 1 December 1995.

4.2.3 System Architecture (SA)

A system architecture is a description—often graphically portrayed—of the systems solution used to satisfy the warfighter's OA requirement. It defines the physical connection, location, and identification of nodes, radios, terminals, *et al* associated with information exchange. It also specifies the system performance parameters. The system architecture is constructed to satisfy operational architecture requirements according to the standards in the technical architecture.

Current plans are to develop the SA for Force XXI in conjunction with a planned series of AWEs. The first increment is the SA for the TF XXI AWE. Following this AWE, system architectures for Division XXI and Corps XXI will be developed.

The SA provides structure for the design and a methodology for implementing Force XXI's system-of-systems environment. It will support assessments of tasks, responsibilities, and risks.

Evaluations of the SA will support estimates on the adequacy and feasibility of the technical and management approach, and a crosswalk against requirements. The SA conveys to both combat and materiel developers the operational considerations and systems solutions that are proposed to meet the stated requirements. The SA can also be the baseline for evaluations of system designs, such as the Applique. Before design is completed, the SA will be assessed to determine if:

- Required functions are implemented in partitioned software.
- Allocation of hardware to units is adequate.
- Hardware component redundancy is adequate.
- ATA is applied.
- Security measures are adequate.
- All interfaces, data flows, services, databases, and network connections are recorded.
- Response times are adequate for warfighter acceptance.
- The form of messages and data is consistent between systems.
- Computer performance and network throughput is adequate.
- Potential performance choke points are identified.

After design efforts are completed and implementation has begun, the SA serves as a basis for measuring progress; developing checklists of actions to be accomplished; and developing test and evaluation plans. It should also be possible to use the SA as a configuration management tool to ensure overall system operational integrity is attained within and between each weapon system platform and node.

Due to the complexity of a system architecture and in order to support ongoing systems engineering efforts, a number of perspectives have been made available or are in the process of being developed to portray the TF XXI System Architecture. These include:

- ***Horseblanket.*** This view is a graphical portrayal which provides a transition between the OA and SA. It depicts the organization, its digitized platforms, and the major systems associated with each platform and/or operational facility.
- **Equipment Matrices**. This spreadsheet view shows the distribution of major digitization equipment (e.g., appliques, digital radios, ATCCS terminals) by TO&E unit, rather than the task organized structure of the *Horseblanket.* It is accessible on the ADO Home Page (http://www.ado.army.mil).
- **Hardware.** This view depicts the identity and location of end-item components, to include hosts, communications devices, routers, servers, and other hardware items.

- **Network Communications and Management.** This view depicts the TF XXI networks, to include topology, communications protocols, and network management.

- **Software.** This view depicts software applications, profiles, and interface standards. It also depicts specific interconnects between systems, to include the HCI.

- **Data.** This view depicts where data originates, is stored, and is distributed. It also defines where specific data elements and standards are used.

- **Security.** This view includes the depiction of the physical security components (e.g., red/black separation and security component allocations) and applicable security policy.

4.2.3.1 System Architecture Development Process

The Force XXI SA is being developed by PEO C3S as the ADO's executive agent and system integrator for the overall Force XXI development process. PEO C3S established the Force XXI Integration Office (FIO) and assigned it responsibility for developing the Force XXI SA, with initial priority on the architecture supporting the TF XXI AWE.

The FIO is following a three-axis approach:

- IPT axis.
- Systems engineering axis.
- SA infrastructure axis.

The IPT axis consists of the effort to capture the information necessary to construct the SA and disseminate its products for feedback and use. Focus of the 16 teams established by the FIO (listed below) is on the *Horseblanket* and related equipment configurations.

- Battle Command
- Mounted
- Dismounted
- Tactical Internet
- Aviation
- Air Defense
- Fires
- Engineer
- CSS
- Medical
- Chemical
- Military Police
- Space
- IEW
- Communications
- Security

The systems engineering axis consists of the efforts to engineer the architecture and validate that it satisfies the OA within the constraints of the TA.

The third axis entails the effort to develop the infrastructure (hardware, software, and database) required to design the SA; support the system engineering efforts; and generate the representations. These representations, beginning with the *Horseblanket*, are developed incrementally and widely distributed for review, comment, and information. More detailed representations, such as the data view, are primarily directed to engineers and computer scientists who are responsible for developing the interfaces between the component systems.

5. ARMY BATTLE COMMAND SYSTEM (ABCS)

ABCS is the integration of command and control systems found at all echelons: from the ground force component commander at the theater or joint task force level to the individual soldier or weapons platform; in an Army force deployed for land combat or conducting peace operations, humanitarian assistance, or operations in aid of civil authorities. ABCS is the integration of battlespace automation systems and communications which functionally link strategic and tactical headquarters. It can also employ a mix of fixed and semi-fixed installations and mobile networks. It is interoperable with joint and multinational command and control systems at upper echelons across the full range of command and control functionality, and is vertically and horizontally integrated at the tactical and operational levels.

ABCS has three major components:

- Army Global Command and Control System (AGCCS).
- Army Tactical Command and Control System (ATCCS).
- Force XXI Battle Command, Brigade-and-Below (FBCB2) system.

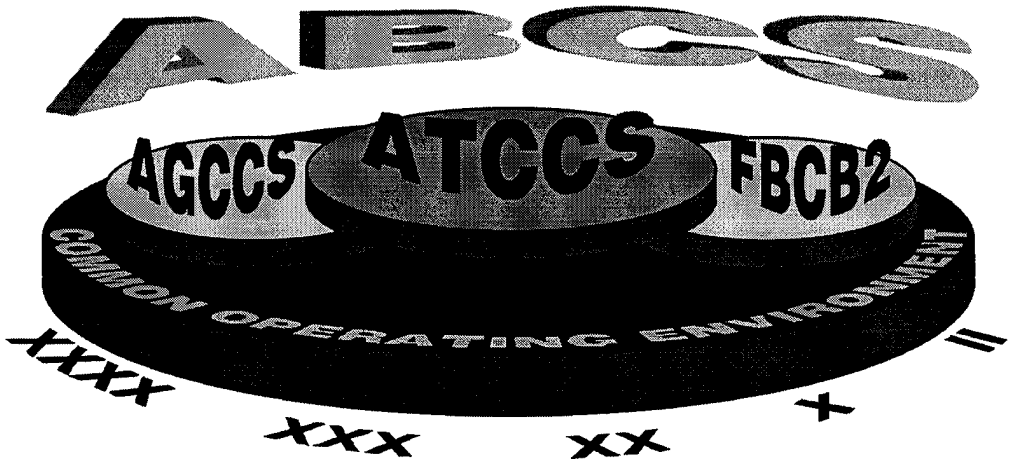


Figure 5-1 Army Battle Command System

5.1 Army Global Command and Control System (AGCCS)

AGCCS is the Army component of the joint GCCS. It is being built from application programs developed by the Army WWMCCS Information System (AWIS), the Strategic Theater Command and Control System (STCCS), and the Echelons Above Corps (EAC) portion of the Combat Service Support Control System (CSSCS). The primary scope of this effort is to evolve these stand alone systems into a suite of modular applications (e.g., logistics, medical, personnel, Theater Army Special Operations Support, mobilization, deployment, Army Status of Readiness and Training, and Transportation Asset Management) that operate within the DII COE. AGCCS modules will interface with common applications and other shared components of the ABCS and with the joint C2 mission applications provided by GCCS.

5.1.1 Army WWMCCS Information System (AWIS)

When the Army is currently called upon to rapidly deploy its forces, AWIS provides the support for the entire operation: from mobilization and deployment through employment and sustainment. AWIS fulfills the Army's strategic C2 requirements for software, hardware, and databases for the implementation of the Joint Operations Planning and Execution System (JOPES) and other Joint Service systems that support the Unified Commands and the Joint Staff. In addition, AWIS modernizes the Army's C2 system, supporting conventional military planning and execution.

AWIS-developed software systems provide the capability for Army commands to

- Analyze courses of action; develop, manage, and support the execution of the Army's responsibilities in the Joint Chiefs of Staff (JCS) War Plans.
- Ensure that the Army's plan is feasible in a global environment.
- Perform status reporting, mobilization, deployment, employment, and sustainment support actions for Army forces supporting conventional joint–military operations.

WWMCCS is a primary national system for both operational and administrative command and control of U.S. Military Forces. It supports the National Command Authority, the Joint Staff, the Unified Commands, and other DoD agencies and activities. WWMCCS is a SECRET *system-high* network with interfaces to joint, Army Theater, National Guard, and Reserve systems.

WWMCCS and the current AWIS are being replaced by GCCS and AGCCS in early FY1996. Since GCCS will operate at the SECRET *system-high* level, the TOP SECRET Support System (TS3) will be implemented until an upgraded GCCS (GCCS-T) is fielded to operate at the TOP SECRET level.

5.1.2 Strategic Theater Command and Control System (STCCS)

Timely, accurate information concerning hostile and friendly forces is essential in reducing decision-cycle time and effectively monitoring execution of operational orders. EAC command and control must not only pass information horizontally to theater staff and subordinate commands, but also interoperate with GCCS, other Service systems, multinational systems, ATCCS Battlefield Functional Area Control Systems (BFACS)/ABCS, and other C2 systems.

STCCS is the Army's means to accomplish EAC C2. It is a peacetime and go-to-war set of software modules that will reside on AGCCS and are designed to assist theater commanders in the execution of crisis and wartime EAC sustainment and operational maneuver functions. STCCS is a user-friendly, highly-adaptable, reliable, and maintainable system. STCCS features ease of modification to meet changing threats and functional requirements, and to enable expeditious insertion of new technology into the system. This is accomplished through adherence to a layered, open system architecture philosophy, employing common hardware and operating system software tied to modular, functional applications through a common ATCCS software system layer. An aggressive software re–use philosophy is also employed.

User experience with fielded software will identify needed capability improvements, user interface changes, and other problems requiring fixes. These will be readily incorporated into STCCS within the constraints of the annual development release cycle.

5.1.3 CSSCS at Echelons Above Corps (CSSCS/EAC)

CSSCS/EAC will consolidate and collate the data required to integrate situational awareness of the CSS mission areas. It will provide strategic and tactical commanders with timely, critical information on ammunition and fuel supplies, medical and personnel status, transportation, maintenance services, general supply, and other field services.

Rapidly changing tactical situations and the intensity of modern warfare demand faster evaluation of force status than is achievable by current manual systems. CSSCS/EAC will give commanders easy access to the resource management, supply, and administrative information required to determine each unit's capability to carry out its mission. The system will also allow commanders to conduct trade-off analyses and evaluate potential courses of action based on different logistical scenarios.

CSSCS/EAC is being designed to improve the planning and execution of CSS C2 operations. A near real-time automated system, CSSCS/EAC will collect, process, analyze, and summarize designated critical information from Standard Army Management Information Systems (STAMIS), including supply, maintenance, ammunition, transportation, personnel, financial, and medical. CSSCS/EAC will consolidate the data and transform it into decision support information for both CSS and force-level commanders.

5.1.4 DII COE Migration Strategy

The Army is committed to migrating its critical C2 mission application systems to the ATA. This will be achieved by developing or migrating mission application (MA) software to use the integrated, shared support services defined by the DII COE. The goal of this migration process is for MAs to eventually consist of only the software necessary to implement mission functionality. All common support functions and infrastructure services required by a MA will be provided by COE services (e.g., mapping and communications).

In order to implement this migration to the COE in compliance with the ATA, system developers will re-engineer and/or retrofit their applications by removing existing program-unique support functionality and replacing that functionality with *calls* for the common services of the DII COE. MA software *calls* for common services will use published DII COE APIs. These APIs will be provided as part of a configuration-controlled On-line Access Library.

The AAE has mandated that all systems must submit implementation plans for complying with the ATA and migration to the COE. The ADO, with ASEO support, is responsible for the review of these plans.

5.2 Army Tactical Command and Control System (ATCCS)

Initially, ATCCS will be linked directly to AGCCS, providing the framework for seamless connectivity from battalion to theater. Objectively, its five tactical C2 systems will merge into a single, coherent, interoperable system binding the combined arms Battlefield Operating Systems together within a unifying COE.

5.2.1 Maneuver Control System (MCS)

The Army is developing and fielding a system for use by commanders and staffs of tactical maneuver units, using a blocked approach. Block II—using Version 10 software running on NDI hardware—is currently fielded to all heavy corps and divisions except the 3rd Mechanized Division. The software for Block III is titled MCS/PHOENIX (MCS/P), since functionality from an experimental program named PHOENIX is being merged into the MCS Version 12.01, the software version currently under development. Block III software will be tested and fielded on Common Hardware and Software (CHS)-2 in FY1996-97. Block IV software will be developed and delivered under a 5-year contract scheduled for award in FY1996. A change to the system name is currently under consideration to reflect recent evolutionary changes in battle command philosophy.

MCS/P will distribute tactical information on the battlefield, allowing a commander to readily access and display current situation reports, intelligence, and contact reports that assess enemy strength and movement, as well as the status of friendly forces.

Through MCS/P, the commander can transmit critical battlefield information such as mission information; courses of action; schemes of maneuver; warning and operations

orders; changes in priorities; and intelligence, fire support, supply status, and air operations requests. MCS/P assists the commander in applying combat power at the appropriate time and place in response to changing battlefield dynamics. In addition, it allows the commander sufficient flexibility to act preemptively to developing situations.

MCS/P databases maintain and display critical situation awareness information on friendly and enemy forces in both text and graphic formats, using data obtained from MCS/P and other BFACS. Using MCS/P decision support graphics—which include map overlays and battle resources by unit—possible courses of action are analyzed, the appropriate course of action is determined, and MCS/P is used to prepare and send warning orders, operations orders, and related annexes.

Exchange of information using MCS/P gives all command posts from battalion through corps the same common picture of the battlespace. Commanders can make decisions that mesh with the decisions and capabilities of other commanders in the network. With the ability to query both local and remote databases, MCS/P also assists in synchronizing the battle.

The MCS/P effort involves the transition of PHOENIX application software modules from the PHOENIX ACT II project into the MCS/P system in preparation for the TF XXI AWE. The procedure for transitioning PHOENIX application software modules is a three-phase process:

- **Phase I** consisted of an architecture evaluation and the porting of relevant application modules to HP UNIX to produce lessons learned.
- **Phase II** consisted of an operational evaluation of PHOENIX functionality with respect to user requirements during Prairie Warrior 95.
- **Phase III** involves the migration of PHOENIX software modules to COE-compliance.

Non-compliant but essential PHOENIX application software modules will be incorporated as evolutionary insertions as they become COE-compliant. Application modules having common functionality within MCS Version 12 and PHOENIX will be consolidated into the MCS/P system. The unified MCS/P functionality will be exercised at Prairie Warrior 96, in a follow-on IOTE, and during the Force XXI AWEs.

IPT Working Groups (i.e., requirements, acquisition strategy/contracts, cost/funding, and testing) are overseeing this transition process. Oversight and review is being performed by an integrated OSD and Services body chaired by ASD(C3I).

5.2.2 Advanced Field Artillery Tactical Data System (AFATDS)

AFATDS is a totally integrated fire support C2 system designed to replace TACFIRE. It processes fire mission and other related information to coordinate and optimize the use of

all fire support assets, including mortars, field artillery, cannon, missile, attack helicopters, air support, and naval gunfire. AFATDS will provide processing capabilities from the corps to the platoon Fire Direction Center.

Through the use of distributed processing capabilities, fire missions will flow through the fire support chain during which target attack criteria will be matched to the most effective weapon systems available at the lowest echelon. The automation provided by AFATDS will enhance the maneuver commander's ability to dominate the battle by providing the right mix of firing platforms and munitions to defeat enemy targets based on the commander's guidance and priorities. AFATDS also expands the fire support commander's ability to control assets and allocate resources.

AFATDS will automate and facilitate fire support planning and current operations. During battle, AFATDS will provide up-to-date battlefield information, target analysis, and unit status, while coordinating target damage assessment and sensor operations.

Integrating all fire support systems via a distributed processing system will create a greater degree of tactical mobility for fire support units and allow missions to be planned and completed in less time. AFATDS will also meet field artillery needs by managing critical resources; supporting personnel assignments; collecting and forwarding intelligence information; and controlling supply, maintenance, and other logistical functions.

AFATDS will interoperate with all fire support systems and ATCCS BFACS, as well as the fire support C2 systems for Germany (i.e., *ADLER*), United Kingdom (i.e., *BATES*), and France (i.e., *ATLAS*).

AFATDS will use modular applications software under development, in conjunction with ATCCS CHS. Major hardware components will be the Fire Support Control Terminal (FSCT) and the Fire Support Terminal (FST).

5.2.3 All Source Analysis System (ASAS)

ASAS is a ground-based, mobile, automated intelligence processing and dissemination system designed to provide timely and accurate intelligence and targeting support to battle commanders. ASAS will provide communications and intelligence processing capabilities to allow sensor and other intelligence data to automatically enter into the all-source database and be simultaneously available at multiple analyst workstations.

Elements of ASAS will provide seamless support to warfighters from theater to battalion levels.

- At EAC, it will be tailored to meet unique theater requirements.
- At corps and division, it will operate from the Analysis and Control Element (ACE), with sanitized intelligence reports and products available at the collateral level.

- At the maneuver brigade and battalion, ASAS workstations will be employed by the S-2 section.

ASAS functions as the IEW subsystem of ATCCS. It provides all-source intelligence fusion which allows commanders and their staffs to gain a timely and comprehensive understanding of enemy deployments, capabilities, and potential courses of action.

ASAS produces ground battle situation displays, disseminates intelligence information, provides target nominations, helps manage organic IEW assets, assists in providing operations security support, and aids in deception and counterintelligence operations.

The Block II development effort will provide an all-source intelligence fusion capability to gain a timely and comprehensive understanding of enemy deployments, capabilities, and potential courses of action. With this knowledge, commanders will have a significantly enhanced view of the battlespace and will be able to more effectively and efficiently conduct the land battle.

Hardware components of the Common Hardware and Software 2 (CHS-2) program will be used in Block II. This new hardware maximizes ruggedness, minimizes weight and cost, while increasing portability and mobility. Interoperability and flexibility will be enhanced through the use of ATA protocols, adoption of the DII COE, and an open systems architecture. Functionality will be enhanced in the areas of all-source and single-source processing; graphics and image manipulation; collection management; auto-sanitation; and the use of digital terrain and automated weather products.

5.2.4 Forward Area Air Defense Command Control and Intelligence System

FAADC2I is an integrated system of weapons, sensors, and command and control that provides C2 and targeting information to air defense weapons systems at the division-and-below levels. It protects maneuver forces, critical command posts, and CS/CSS elements from low–altitude air attack. The system uses CHS processors and operating systems, with data communications provided by the Army Data Distribution System (ADDS), SINCGARS, or dedicated digital radio links.

Integrating sensor inputs from various sources, FAADC2I provides early warning, targeting, and control information to FAAD and supported units. An *area of interest* air picture is developed and air tracks are identified using automated and manual means. Threat tracks cause alerts, with fire units automatically cued to the targets. FAADC2I integrates battlespace control measures in relationship to the air picture, which is displayed to fire units to enhance acquisition of hostile tracks by the weapons systems.

The initial development effort of FAADC2I is concentrating on *engagement operations*, which are real-time actions supporting aircraft engagement. The system will begin encompassing more *force operations* functionality (e.g., all unit plans, support, and day-to-day operations) as the program matures.

At the corps level, FAADC2I will be integrated with PATRIOT, HAWK, and future Corps SAM and their associated C2 systems into the comprehensive Air and Missile Defense (AMD) system. Within AMD, essential C3I operational functions will be distributed among Air Defense Tactical Operations Centers (ADTOCs), sensor nodes, and fire units throughout the depth of the battlefield, providing the capability to acquire, process and distribute information necessary for the planning and coordination of AMD operations. The ADTOC will serve as the AMD link to ABCS and joint/allied C3I systems. It will process and distribute the information required to direct AMD forces and synchronize the their actions with the maneuver commander's concept of operations.

The objective AMD system will be achieved through an evolutionary process.

- **Block I**: the current FAADC2I and the prototype Air Defense Brigade TOC.
- **Block II**: improvements to the PATRIOT Battalion TOC and the battalion-level Improved C3I (IC3I) capability of FAAD. It will also provide a battalion/battery-level IC3I capability for the Theater High Altitude Air Defense System (THAAD).
- **Block III**: the objective system and reflects the fielding of the ADTOC capability and the required vertical and horizontal interfaces to ABCS.
- **Block IV**: reflects P3I.

5.2.5 Combat Service Support Control System (CSSCS)

CSSCS will consolidate and collate the vast quantities of data required to integrate situational awareness within the CSS mission areas. CSSCS will provide tactical commanders with timely, critical information on ammunition and fuel supplies, medical and personnel status, transportation, maintenance services, general supply, and other field services. CSSCS, as a component of ATCCS, has essentially the functionality as described in Section 5.1.3 (CSSCS/EAC), with the exception that data output will be tailored for brigade, division, or corps commanders, as appropriate.

5.2.6 ATCCS DII COE Migration Strategy

With the advent of the DII, the Army has acted vigorously to integrate CHS products into the COE. As a result, current CHS procurements include COTS modules which are COE-compliant and which are being migrated into the ATCCS systems as they are individually upgraded. In addition, many COE elements will be incorporated into the CHS program and will be provided to the ATCCS PMs as a coherent software package for incorporation into the ATCCS systems. The Army recognizes that this must be an evolutionary process, given the resource constraints which characterize the current and forecast defense budgets. To realize the full potential which the COE offers, MA software which cannot function within the COE must also be modified or rewritten to use the integrated, shared support services provided by the COE.

Army migration strategy involves the removal of existing support functions and their replacement with the appropriate/matching common function. When a mission application is undergoing significant modification and/or enhancement, developers must utilize COE components whenever generalized support functions are required and appropriate COE components are available. In instances where the appropriate functionality is not yet available in the released version of the COE, surrogate software modules that will perform the required support function may be used. This surrogate software will be provided to DISA as candidates for incorporation into the COE. Surrogate support software must still be replaced with the appropriate baseline COE modules as they become available.

Surrogate software must also comply with the ATA. If the COE contains published APIs for a specific support function, but the underlying modules do not yet contain the complete required functionality, the application developer should acquire the surrogate code using the public API as an interface specification for the surrogate support functionality. This supports a simplified migration from the surrogate code to the baseline COE module when it becomes available. These surrogate support modules may also be proposed for integration into the COE baseline. PM CHS will maintain configuration management control over surrogate code developments to ensure that multiple similar surrogates are not developed, and that those which are developed are compliant with the DII COE architecture.

The Army is currently working with DISA to expedite migration to the DII COE. For Army systems/platforms at or approaching COE compliance, the transition will be accomplished by using common build tapes. In other cases, the technical challenges associated with the transition will be addressed by an integrated DISA/PEO C3S team. The team will specifically address issues such as documentation, scaling the COE for limited-capability Army platforms, heterogeneous environments, and Army-required COE modules. The result will be an extension of the COE and a wider applicability of its products.

Under the AAE mandate that systems must submit implementation plans for compliance with the ATA and migration to the COE, the PMs for the ATCCS systems have submitted their initial draft plans for migrating to the COE and the other applicable standards of the ATA. The ASEO, in coordination with the ADO, will monitor the plans to ensure that the process remains coherent across the spectrum of Force XXI activities.

5.3 Force XXI Battle Command, Brigade-and-Below (FBCB2)

FBCB2—more fully described in Section 6.1—will provide situational awareness and command and control to the lowest tactical echelons. It will facilitate a seamless flow of battle command information across the battlespace, and will interoperate with external command and control and sensor systems, such as ATCCS. The end result will be a vertical and horizontal integration of the digital battlespace and the brigade-and-below tactical unit levels.

The FBCB2 system is comprised of:

- Appropriate category of applique or embedded system hardware.
- FBCB2 software—architecturally compliant with the DII COE.
- Position navigation and reporting capability (e.g., Global Positioning System (GPS) or an embedded position-navigation (POSNAV) capability).
- An interface to a terrestrial communication system (e.g., SINCGARS and/or Enhanced Position Location Reporting System (EPLRS) radio) or to a satellite communications system for operations over long distances or rugged terrain.
- A combat identification capability (e.g., a BCIS capability).

Functionally, the FBCB2 system will support lower–echelon battle command tactical mission requirements including:

- Real-time situational awareness for commander, staff, and soldiers.
- Shared common picture of the battlespace.
- Graphical displays, with friendly and enemy unit locations.
- Target identification.
- Integrated logistics support.
- Communications/electronics interfaces with host platforms.

6. IMPLEMENTATION STRATEGY

The digitization implementation strategy is comprised of four thrusts.

- Developing C2 software initially focused at brigade-and-below.
- Establishing a seamless communication infrastructure called the *Tactical Internet* that will evolve into an enhanced Warfighter Information Network (WIN).
- Migrating Army battlespace systems onto the *Tactical Internet* by means of standardized protocols, data standards, and message exchange formats, incorporating FBCB2 functionality where applicable.
- Developing a Battlefield Information Transmission System (BITS) that will augment the near-term implementation of the *Tactical Internet* with emerging commercially-based technologies that—in the far-term—will allow for the increased information flow necessary to support a fully digitized force.

These thrusts, which are conducted in accordance with the Technical, Operational, and System Architectures, are in full compliance with DoD architectural guidance and will be executed in the three phase process described in Section 7, Acquisition Strategy. The intent is to quickly digitize by employing current technologies to acquire, exchange, and process critical information throughout the battlespace and to evolve this capability to reflect insights gained from AWEs and opportunities for technology enhancements.

6.1 Thrust 1 - Force XXI Battle Command, Brigade-and-Below (FBCB2)

FBCB2 provides near-term C2 capabilities to Force XXI units at brigade and subordinate echelons. The FBCB2 system is comprised of hardware, software, and databases being acquired under the Applique and other programs. FBCB2 interfaces with:

- Items already found at brigade-and-below echelons. Examples of these are components of ATCCS and C4I capabilities embedded in weapons systems/platforms.
- The Army *Tactical Internet*, which is Thrust 2 of the Army's Implementation Strategy and is discussed in Section 6.2.

One of the most important aspects of this effort is the development of software and database capabilities which are common and seamlessly interoperable across all systems at these echelons. The FBCB2 software suite, which re–uses and incorporates existing commercial and government software wherever practical, will meet the open systems standards found in the ATA. The FBCB2 software suite is also being developed for forward compatibility with the mainstream of commercial hardware and software developments in order to facilitate the insertion of new technology as the Army evolves to Force XXI. FBCB2 software will incorporate essential

functions from the M1A2's Inter-Vehicular Information System (IVIS) and from the Brigade-and-Below Command and Control (B2C2) prototype. New functionality is being concurrently developed, based on requirements contained in the FBCB2 UFDs.

6.1.1 FBCB2 Software Functionality

FBCB2 software functionality is contained in operating system, utility, and mission applications software. This software will be modular; have formally defined and openly published APIs; and will be scaleable across a range of host hardware platforms.

6.1.1.1 Common Operating Environment Compliance

FBCB2 will have an operating environment that is compliant with the DII COE. It will consist of operating system and support software modules which are either reused directly from the DII COE discussed in Section 4, or are functionally compatible with it. The Army will re–use COE modules where possible. Work has begun to determine if necessary COE modules can be scaled-down to function satisfactorily on man-portable digitized systems—such as the Dismounted Soldier System Unit (DSSU)—and selected embedded weapons system processors. All software developed by the FBCB2 Program will be DII COE-compliant to the extent possible; designed for use by either strap-on or embedded programs; and used as necessary to extend the COE through the formal COE extension process.

6.1.1.2 Situation Awareness

Situation awareness is provided by collecting, integrating and displaying a common *picture* of the battlefield that is consistent in both time and space at each user display. MA software being developed for FBCB2 situation awareness allows the geographical location of individual soldiers, weapons/platforms, command posts, and other operational facilities to be collectively presented on a display. Because the Army *Tactical Internet* is a true, seamless internet based on the world-wide Internet model, it is possible to communicate each individual geolocation to every FBCB2-equipped user within the *Tactical Internet.* Addressing mechanisms allow geolocations to be flexibly and selectively communicated, and situation awareness software functionality will contain the necessary filters and *roll-up mechanisms* for each user to be able to selectively display only the locations of units of interest.

6.1.1.3 Operational Control

One of the methods by which operational control is achieved is through the transmission and receipt of orders, reports, and data in a timely manner. The VMF messaging function of FBCB2 software provides a key mechanism for effecting that exchange, using a set of 51 joint-approved VMF messages. Each FBCB2-capable system will have the ability to automatically or manually compose, edit, transmit, receive, and process either the full set of these messages or a subset which is specific to the mission profile of that system. The initial VMF message set of 21 messages was developed specifically for the TF XXI AWE and will be expanded for use in the Division XXI and Corps XXI AWEs. It provides the ability to communicate orders, reports, and data in near real-time over the bandwidth-restricted networks found at brigade-and-below echelons. The VMF

messaging software also provides the ability to insert and extract data from these messages for automatic insertion or update of tactical databases.

6.1.1.4 System Management and Control

FBCB2 will be a complex system involving over 1,000 computers in each maneuver brigade, all tied together in a single seamless network. Since it is not possible for this system to start up, operate, and gracefully degrade of its own accord under all conditions without human intervention, FBCB2 software will provide the capability to initialize, control, and conduct an orderly shut-down of the FBCB2 system. Capabilities will be provided in the areas of:

- **System Management:** tasks such as loading network initialization data, maps, cryptographic keys, and network addresses prior to an operational deployment.
- **Communications Planning:** tasks such as laying out networks, making frequency assignments, and specifying address/circuit assignments/procedures prior to deployment.
- **Network Administration:** background tasks such as the monitoring and control of network resources and configuration once operations have commenced.
- **Network Management:** real-time tasks such as dynamic network reconfiguration, timekeeping, and circuit deactivation during operations.

6.1.2 Functionality Implementation of FBCB2

6.1.2.1 Applique

Use of appliques is intended to provide C2 capabilities to platforms that either have no embedded C2 capability or whose existing capability is inadequate to meet emerging user requirements. For a platform lacking an embedded digital capability, it will be *appliqued* with:

- Appropriate applique hardware.
- FBCB2 software.
- Position/navigation capability.
- An interface to a SINCGARS and/or EPLRS radio.
- BCIS (not included in all platform packages).

6.1.2.2 Army Tactical Command and Control Systems

As discussed in Section 5, ATCCS systems are in the process of migrating to the DII COE. Since FBCB2 functionality is also based on use of the COE, selected FBCB2 functional components will be provided for incorporation into ATCCS systems in the near–term. In the far–term, core FBCB2 functionality and other mission applications will be migrated to ATCCS systems.

6.1.2.3 Embedded Systems

Many Army systems have an embedded C4I capability, including the M1A2 Abrams, the M2A3 Bradley, the AH-64D Longbow Apache, and the OH-58D Kiowa Warrior. At a minimum, the Army plans to integrate FBCB2 software functionality into these platforms sufficient to generate and receive an appropriate subset of the VMF message set.

6.1.2.4 Other Systems

The Army is working with the Navy, Air Force, and Marine Corps to provide interface documentation, FBCB2 software modules, and/or complete applique sets for use in various warfighting experiments, as appropriate to the needs of the user.

6.2 Thrust 2 - *Tactical Internet*

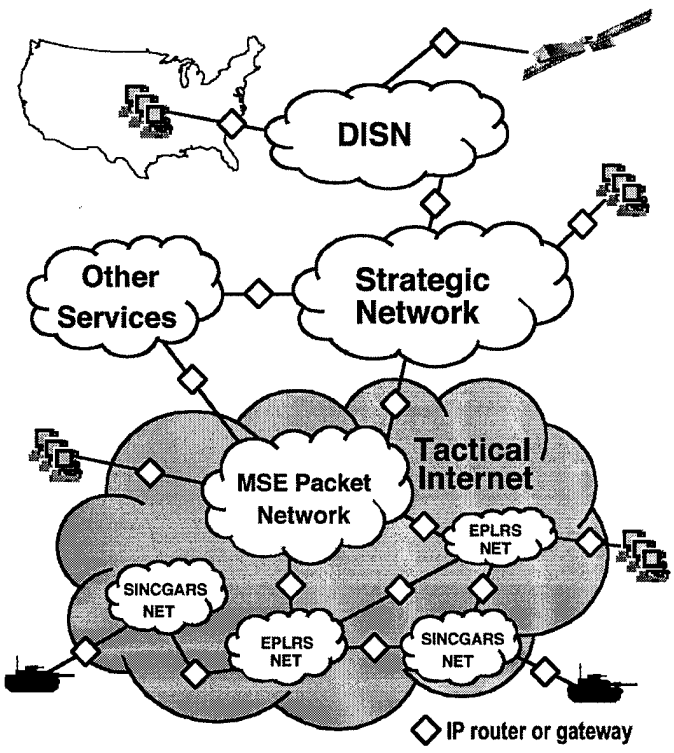


Figure 6-1 Integrated Digital Information Network

One of the top priorities of the Army in digitizing the battlespace is to provide command and control capability throughout the force. This requires a horizontally and vertically integrated digital information network that supports warfighting systems and assures command and control decision cycle superiority. The network must provide reliable, seamless, and secure communi-cations connectivity for all Army tactical users

The *Tactical Internet* is the term used to describe this integrated battlespace communications network The term is appropriate due to functional similarities to the commercial Internet and because the communications infrastructure supporting the *Tactical Internet* is based on Internet technology. A key feature is the ability to exchange VMF messages using the commercially-based Internet Protocol (IP), which is mandated in the ATA and is common across all segments of the *Tactical Internet.*

As depicted in Figures 6-1 and 6-2, the initial digital communications system will consist of a space-based segment, an EPLRS-based backbone, a SINCGARS CNR segment, and a Mobile Subscriber Equipment/Tactical Packet Network (MSE/TPN) segment—all integrated via routers.

The integrated digital transport capability of these communications segments is key to moving information among the Force XXI nodes and platforms. The communications infrastructure is focused on achieving seamless information transfer horizontally and vertically across the battlespace. This is achieved through the employment of commercial Internet technology (e.g., IP routers) and open standards protocols (e.g., TCP/IP). COTS IP-based routers (e.g., Tactical Multinet Gateways (TMGs) and Local Area Network (LAN) routers) and Internet Controllers (INCs)—which are single circuit card, militarized Internet-based routers—provide the ability to send messages between any segment of the tactical battlespace network. While INCs are physically incorporated into a SINCGARS mount, they provide a *host* and an EPLRS interface, as well as a SINCGARS interface.

Enhanced versions of the three primary Army tactical communications system segments—EPLRS, SINCGARS, and MSE/TPN—will move the ever-increasing amount of digital data associated with command and control applications employed within the modern battlespace. Capabilities will also exist to interface the *Tactical Internet* to commercial and military satellite communications (SATCOM), providing unprecedented capacity and access to lower–echelon units.

- SINCGARS enhancements include reduced cosite interference; improved error detection and correction; reduced network access delay; and a GPS interface to obtain accurate time and position location. Collectively, these improvements will greatly extend the effective data communication range and increase information throughput from 1.2 kbps to 4.8 kbps. Test results indicate that the SINCGARS SIP radio will be able to reliably pass data at 4.8 kbps up to a range of 35 kms in a benign environment.

- The EPLRS system now incorporates Very High Speed Integrated Circuit (VHSIC) technology which will increase the throughput of individual EPLRS users from 4 kbps to 12 kbps.

- The MSE/TPN program is upgrading its routing protocols from the Exterior Gateway Protocol (EGP) to the Border Gateway Protocol (BGP). This change will substantially reduce the bandwidth required to exchange routing information between routing devices in different networks.

The *Tactical Internet* supports several key services. These services include functions such as electronic messaging, directory, network management, and security. These services are integral to the value of the *Tactical Internet* in support of the warfighter. As new host-based services are added—such as DMS electronic mail service—their supporting system components will be folded into the *Tactical Internet.*

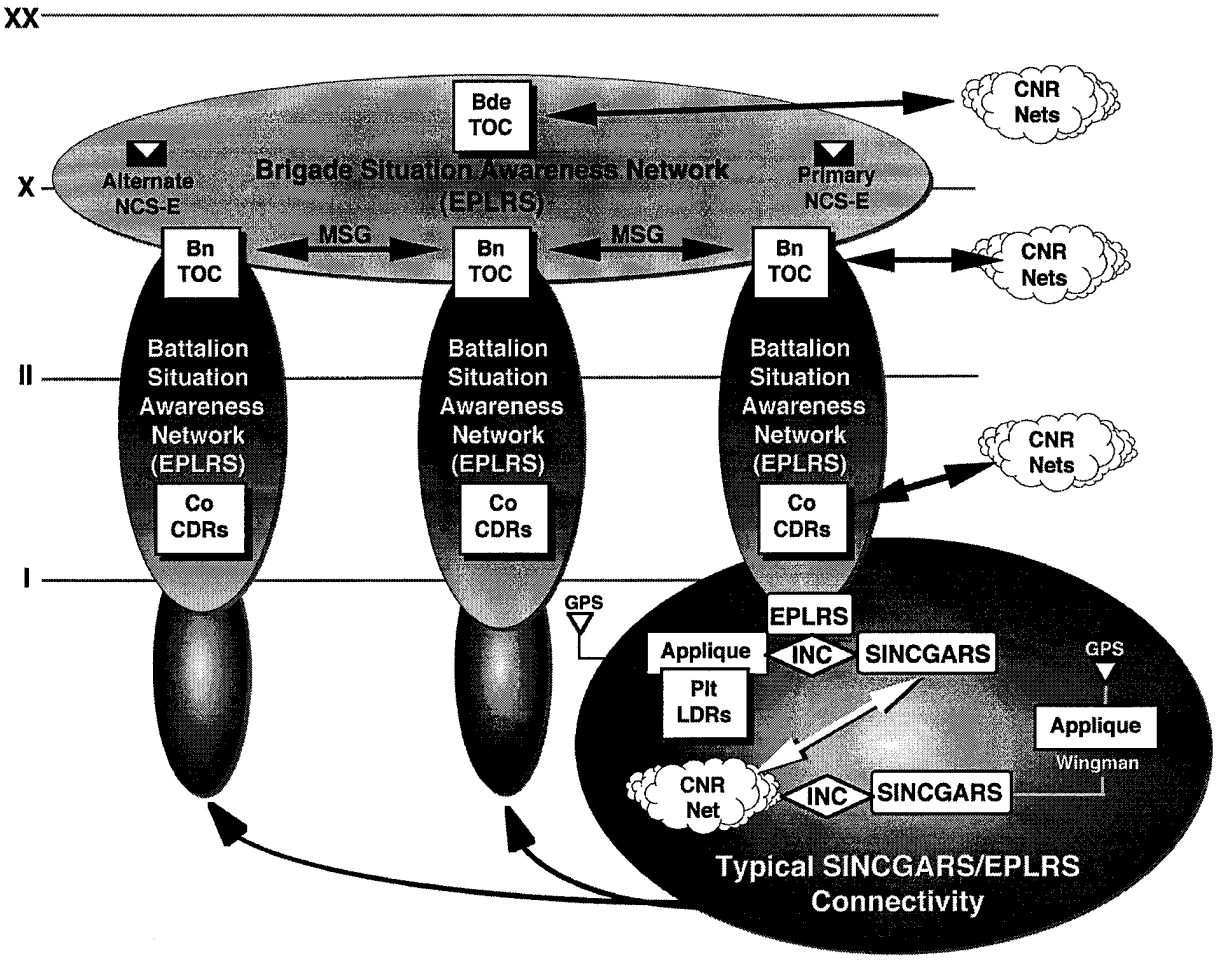


Figure 6-2 Simplified *Tactical Internet* Components at Brigade Level

Security is an important service within the *Tactical Internet*. Because of the concern for security, the *Tactical Internet* will initially be operated as a *SECRET High* system. Since all directly-connected host computers will be capable of operating up to the Secret level, direct connections to the commercial Internet cannot be permitted. There is, however, a great deal of interest in the new end-to-end encryption devices that will permit Unclassified users to use the *SECRET High Tactical Internet* to access Unclassified computers connected to the commercial Internet. This capability is of particular importance to CSS users, who typically use Unclassified applications and data, and need to communicate in a split-based mode with large computer systems in CONUS. The availability of multi-level security services will enable greater network flexibility. As these services are realized and integrated into the *Tactical Internet*, the issue of a *SECRET High* network infrastructure will be revisited.

Another key component of the *Tactical Internet* is technical control. The Integrated Systems Control (ISYSCON) program is developing the capability to technically control networks at brigade-and-above level. Since TMGs and INCs must also be technically controlled, additional ISYSCON capabilities in the form of Automatic Network Managers (ANMs) are being added to control the *Tactical Internet* at brigade-and-below. The management protocol for the ANM will

be Simple Network Management Protocol (SNMP), with SNMP agents implemented by communications elements. In some cases, however, proxy agents will be used (e.g., SINCGARS and EPLRS proxy agents will be hosted on the applique).

The Signal Center (SIGCEN), in conjunction with CECOM, is investigating the operational and training impact of the *Tactical Internet.* A series of BLWEs, AWEs, and Joint Warfighter Interoperability Demonstrations (JWIDs) will provide an experimental basis to:

- Assess personnel requirements.
- Determine needed training and skill levels.
- Provide a venue for ascertaining and recommending changes to communications tactics and procedures.

PEO C3S, with the support of CECOM and SIGCEN, is responsible for developing the *Tactical Internet* in accordance with the SA.

Improvements to components comprising the SA are needed to make the *Tactical Internet* viable. The use of commercial Internet protocols provides the required level of seamless connectivity between the different networks, but Internet protocols increase data capacity requirements because additional header information must be added to each message. The Internet routers exchange routing and status information, which also increases data capacity requirements. Even with the improved data capacity of SINCGARS, EPLRS, and MSE, these systems provide relatively small communications trunks compared to fixed-site commercial systems. A comprehensive modeling and simulation effort is therefore required to determine the optimum parameters for the use of Internet protocols in a dynamic military environment featuring relatively few communication links.

6.3 Thrust 3 - Integration of Battlefield Operating Systems

The integration effort will link the components of ABCS to individual weapons systems, creating a seamless network from the soldier through the tactical and operational levels to the sustaining and strategic level. Technical integration of legacy systems and embedded and non-embedded digital capabilities into a system-of-systems presents many challenges.

6.3.1 Embedded Systems

Embedded systems are digital system components providing functions and processes which are integrated into a hardware platform to such an extent that they can not be considered as discrete entities during development, testing, or production of a system. Examples include fire control, position/navigation, diagnostics, and communications equipment installed on the M1A2 Abrams, AH-64D Longbow Apache, and OH-58D Kiowa Warrior. The software and hardware of these platforms may also perform common battle command functions such as providing situation awareness, using common digital terrain data, and receiving/transmitting digital messages.

Some embedded digital systems are wholly contained within a platform, with standards and protocols for their internal connectivity defined by the PEO. The PEO must consider cost when applying standard development concepts such as growth, open system architectures, flexibility, and interoperability with other platforms.

Modular, multi-function hardware designs are being adopted. Emerging technology affords the opportunity for a significant shift away from single-purpose designs toward multi-purpose alternatives in which functions are implemented on removable, upgradable circuit cards, microchips, or in the software.

Embedded digital systems that interact with dissimilar weapon systems or C2 nodes must at least use common message sets. Digital communications, standard data protocols, icons, and applications are required to pass the same information for applications such as overlays, calls-for-fire, and spot reports. The ATA provides specific requirements in this area, which will be documented in Interface Control Documents (ICDs).

Embedded digital systems already in the inventory or programmed for future fielding are part of the SA. The primary integration challenge resides at the lower echelons, where existing legacy systems were originally developed to provide vertical *stovepipe* information flows in support of specific battlefield functional areas. As such, the Applique contractor has developed system/subsystem segment ICDs for platforms to be digitized. The ICDs will document interfaces to existing platform power, MIL-STD 1553 data bus, communications, navigation, and sensor subsystems as appropriate.

The AAE has mandated compliance with the ATA by all PEOs and PMs, to include those who are developing platforms with embedded digital systems. In practice, this mandate requires the PEOs and PMs to:

- Provide support to PM Applique, which will include: providing technical data packages to the applique prime contractor for development of installation kits and interfaces; providing technical assistance in evolving/defining system integration requirements; and making platforms available for technical integration testing.

- Develop plans laying out a strategy for migrating their systems to the ATA, to include MIL-STD-188/220A, VMF, C2 Core Data Model, and DII COE.

- Integrate appropriate FBCB2 software supplied by PEO C3S as an additional application, sharing the host processor with existing weapons system–specific applications.

- Develop and document the program funding and schedule changes required to support migration to the digitized force IAW the acquisition strategy.

- Incorporate digitization test criteria in system TEMPs.

- Address the critical elements of the digitization initiative in all program reviews.

6.3.2 Legacy Systems

Many legacy systems will be a part of the digital battlespace. They present a wide range of integration issues associated with protocols, data standards and message exchange. For example:

- ATCCS currently uses USMTF as its primary message exchange system.
- The Interim Fire Support Automated System (IFSAS) and TACFIRE use the TACFIRE protocol and message set.
- The Marine Corps Tactical Command and Operations (TCO) System employs the Marine Tactical System protocol and message set.

To reduce the risk associated with development of FBCB2 software and the *Tactical Internet*, both will be baselined on the world-wide Internet protocol suite (i.e., TCP/IP). Additional baseline elements include the TF XXI VMF TIDP and its associated data communications protocols, such as MIL-STD 188-220A.

The ADO is working with the various legacy PEOs and PMs to obtain forward compatibility with FBCB2 software and the *Tactical Internet*. For example:

- PEO C3S is developing a USMTF-to-VMF translator to achieve interoperability as ATCCS migrates to the Joint VMF.
- PEO C3S has implemented the MIL-STD 188-220A and EPLRS X.25 protocols.
- PM AFATDS is now implementing the TF XXI VMF fire support messages.

SINCGARS SIP radios, applique hardware, and FBCB2 software may be provided as an interim capability for cases in which schedules, funding or technical considerations do not allow near-term integration and interoperability. Backward compatibility will be selectively implemented.

6.3.3 Sustaining Base Systems and Intelligence Systems

Although the initial focus of digitization has been on C2 systems, the Army is also digitizing its Army battlefield personnel and logistics processes—the sustaining base systems—and is taking steps to more fully integrate these systems and the tactical intelligence systems into the digitized force. This poses two unique challenges. The first is associated with security, and the second with split base operations.

6.3.3.1 Multi–Level Security

While the Army's tactical communications backbone and other battlefield automated systems generally operate at the SECRET level, sustaining base systems normally operate at the UNCLASSIFIED level, while certain intelligence systems operate at levels more restrictive than SECRET.

In the far–term, the Army plans to address this multi–level security challenge by migrating its communications backbone to the Defense Goal Security Architecture (DGSA) in harmony with the Defense Information System Network (DISN), using components (e.g., Fortezza) developed under the Multilevel Information Systems Security Initiative (MISSI). In the near–term, the Army plans to use In-Line Encryptors (INEs)—such as the Network Encryption System (NES) and the Tactical End-to-end Encryption Device (TEED)—that will allow sustaining base and intelligence systems to use the *Tactical Internet* by *tunneling through.*

6.3.3.2 Split Base Operations

The evolving split base concept envisions some portion of sustaining base and/or intelligence assets either remaining at their normal peacetime location or deploying to a safe haven some distance from the battlefield. The success of this concept hinges, in part, on the ability of forward-deployed units to *reach back* via responsive communications to their stay-behind elements, and this implies a communications capability able to support this *reach back* requirement.

When connected to the DISN through a Standardized Tactical Entry Point (STEP), the *Tactical Internet* will provide seamless data communications from the forward deployed to the stay-behind elements. The Army also plans to exploit commercial communications capabilities using Trojan Spirit II and Tri-band satellite communications terminals, as well as the high-data rate capacity now emerging under the Battlefield Awareness and Data Dissemination (BADD) program. The Army must also modernize its *power projection platforms*—the fixed installations at the stay–behind end of split base operations.

6.4 Thrust 4 - Battlefield Information Transmission System (BITS)

As more users and increasingly-complex systems are added to the battlespace array, the *Tactical Internet* will be unable to handle the data transmission load. In the next 2–5 years, this shortfall will be absorbed by adding a Near Term Digital Radio (NTDR) to replace EPLRS. For the far–term, the BITS program is developing technologies for much greater information throughput.

The technology programs being pursued by the BITS program are described below. Proposed product availability dates for insertion into the major AWEs are shown in Figure 6-3.

The strategy for acquiring a BITS capability is based on the following three-phase program:

- **Research and Development Phase** (approximately five years): Technology base programs and demonstrations (e.g., ACT II, ATDs.) will be used to identify candidate technologies; evaluate products in a laboratory environment; perform modeling and simulation; and perform experimental testing in a user environment.

- **Leave-Behind Phase** (approximately two years): Products will be left with operational units that participated in first-phase evaluations so they can develop corresponding TTP concepts and provide the acquisition community with requirements feedback.

- **Fielding Phase** (approximately two years): PEOs/PMs will develop system requirements from the operational requirements established during the second phase and acquire the required capability.

PRODUCT	QUANTITY	TF XXI	DIV XXI *	Corps XXI*	FY 99
Near-Term Data Radio/Surrogate Data Radio	24 SDR Up to 400 NTDR (option) Up to 900 NTDR (option)	X		 [X]	
Asynchronous Transfer Mode	11 ATM Switch (MSE) 4 Low Rate ATM Switch 7 Multimedia Workstation	X X X			
Tactical End-to-End Encryption Devices	30 TEED	X			
Terrestrial Personal Communications Systems	LMR:1Base Station/50 Handsets 2 MSE Interface (each) Hybrid CDMA: 2BS/50 Handsets	X X	 X X		
Global Broadcast Service	1 Uplink, 8 Downlinks 1 Program Center 1 UAV Payload 1 OTM Antenna	X	 X	 (X) (X)	
High-Capacity Trunk Radio	4 HCTR (10 Mbps) 4 Static HCTR (45 Mbps) 4 OTM Antenna		X	 X	 X
Airborne Relay	1 Abn Relay (45 Mbps) 1 Abn Relay (155 Mbps)		X		 X
Satellite Personal Communications System	1 UAV Payload, 25 Handsets Up to 100 Universal Handsets		X		 X
On-the-Move Antenna	1 OTM Antenna (45 Mbps)			X	
Radio Access Point	1 Static RAP 1 OTM Antenna (Mobile RAP)			X	 X

(X) Development complete, but not funded for AWE
* Subject to change based on Oct 95 decision on downscoping Division and Corps AWEs

Figure 6-3 BITS AWE Product Insertions

6.4.1 Surrogate/ Near–Term Digital Radios (SDR/ NTDR)

Under the SDR BAA, CECOM will provide approximately 24 SDR systems. The concept of operations for the TF XXI AWE is to equip a portion of the brigade with the SDR BAA field models to form a small digital radio net. The goal of the experiment will be to determine its effectiveness in passing high-volume digital traffic through a network in a battlefield situation.

The NTDR system will have an open hardware, software, and system architecture. An NTDR testbed will be established in the DIL at CECOM for inserting technology from SPEAKEASY and other programs. Through the process of technology insertion, the NTDR may ultimately provide the full range of functions and capabilities required of the SDR.

6.4.2 Asynchronous Transfer Mode (ATM) Technology Integration

Emerging high-data-rate services and applications (e.g., video) cannot be effectively supported by the existing MSE/Tri-Service Tactical (TRITAC) system. ATM technology has the potential to support these and other wideband services, but was designed for use in low bit-error-rate, fiber optic-based static networks. Effective use of ATM technology in a tactical environment will require that forward error correction, low-rate survivable protocols, bandwidth allocation, signaling, and wireless ATM areas each be adequately addressed before ATM is ready for use with the new High-Capacity Trunk Radios (HCTR).

ATM experiments conducted during Unified Endeavor in April 1995 will serve as the program baseline. In that exercise, seven ATM switches were installed into MSE shelters, enabling MSE voice traffic to be combined with data traffic over the existing MSE backbone network.

This and other field trials have shown that while ATM technology can be used in certain tactical applications, many technical issues must be resolved before ATM technology can be deployed effectively in a tactical network.

- The first phase of the program will provide incremental improvements to the MSE system within the existing bandwidth constraints.

- During the second phase, the effort will concentrate on issues associated with introducing high-bandwidth radios into the tactical battlespace. At the end of this phase, a functional specification for a replacement to the existing MSE system will be provided.

6.4.3 Tactical End-to-End Encryption Device (TEED)

TEED is an encryption device used to provide end-to-end security for Force XXI data users. As long as the MSE/TPN remains at its current *SECRET High* security level, TEED would be used by:

- Unclassified logistics users who need to use the MSE/TPN as a common carrier.

- IEW users whose security needs exceed the SECRET level of the MSE/TPN.

In the first instance, TEED is used to protect the base-level Secret users from users working at lower classifications. In the second, TEED protects the higher-level Top Secret users from the base network. TEED is designed to protect both of these applications. Further development is needed to produce a TEED that will encrypt ATM and IP traffic. The National Security Agency (NSA) is investigating the new *BATON* encryption algorithm for this use.

6.4.4 Terrestrial Personal Communications Systems (PCS)

Research and development performed in the area of terrestrial PCS is a cooperative effort between the ARPA-funded Commercial Communications Technology Testbed (C2T2) program and the CECOM Commercial Communications Technology Laboratory (C2TL) and Digital Battlefield Communications (DBC) ATD programs. PCS capabilities developed under these programs will be demonstrated during the TF XXI AWE.

The Land Mobile Radio (LMR) system provides intermixed digital voice and data transmission over multiple 9,600 baud, half-duplex channels. Handheld Personal Digital Assistants (PDAs) and generic laptop x486 computers are interconnected via this system. GPS receivers and heads-up displays are also integrated with the computing devices.

Hybrid PCS is the second-phase system under the C2T2 program. It is expected that this second system will have smaller (transportable) base stations; better hand-off and *peer forwarding*; more users per channel; higher data rates; and lower transmit power. Broadband code-division multiple access (CDMA) technology is being explored for this system.

A key piece of the demonstrations scheduled in conjunction with the TF XXI and Division XXI AWEs is the interface to MSE. Because current LMRs only have an interface to the public switched telephone network, a more complex interface is needed for MSE. This interface will be developed under the DBC ATD.

6.4.5 Army Direct Broadcast Satellite (DBS)

Commercial DBS systems offer the potential for low-cost, wideband data and video dissemination. Unfortunately, these systems are geographically limited to CONUS; are designed specifically for the home user; use commercial frequency bands; and are nearly at maximum capacity. This project, in coordination with the Joint Global Broadcasting System (GBS), will develop an Army DBS system providing the flexibility required to support operations while maximizing the benefit of low-cost commercial developments.

Three commercial DBS terminals will be acquired, modified to work with standard Ku-band antennas, and integrated with Sun workstations to provide an uplink/downlink capability. A single Army DBS programming center will be established to consolidate, schedule, and control data/video dissemination. An airborne DBS transponder will be developed and demonstrate a global capability for in-theater data dissemination under direct control of the theater commander. Finally, the capability to receive DBS data on a moving platform will be explored.

6.4.6 High-Capacity Trunk Radio (HCTR)

HCTR will serve as the next-generation line-of-sight radio for MSE. It will provide a trunk radio capable of a minimum data rate of 45 Mbps to support ATM switching. As an integral part of the Radio Access Point (RAP), the HCTR will also extend wideband integrated communications services to highly mobile forces.

The HCTR program is a technology-based, advanced development initiative to explore and develop technologies supporting a wideband trunk radio with the capability of operating while on-the-move. The program will include the evaluation of a COTS synchronous optical network (SONET)-based radio, starting with the delivery of the radio in November 1996 and concluding with a report in September 1997. Concurrent with the COTS SONET radio experiment, an accelerated procurement will be conducted to provide a near-term wideband radio, HCTR(-), with a performance goal of 10 Mbps and 20 Km range for near-term ATM upgrades to MSE. The objective HCTR will be capable of providing 155 Mbps operation in a static mode, and 45 Mbps in an on-the-move mode. Four on-the-move HCTRs are planned for delivery in early FY99.

In the stationary mode, the HCTR will provide a wideband multi-channel trunking capability for MSE. It will act as an upgrade replacement for the current AN/GRC-226, providing wideband backbone and extension links for ATM-equipped MSE switching assemblages. In the on-the-move mode, the HCTR will be operated as an integral part of the mobile RAP. As part of the RAP, the HCTR will connect various narrowband tactical systems—including SINCGARS, EPLRS, NTDR, and MSE—to the wideband point-to-point backbone network.

6.4.7 Airborne Relay

Current extended-range communications are heavily dependent on satellite links and terrestrial networks, presenting a number of operational limitations in many parts of the world. This project will develop an airborne relay capability providing a wideband communications range extension, supporting the HCTR and RAP programs. The wideband airborne relay will also be part of the UAV communications payload suite.

6.4.8 Satellite Personal Communications Systems (PCS)

Satellite PCS will provide worldwide communications via networks of low–earth orbiters using handheld units. Systems are expected to support voice, facsimile, data and paging communications. This program will investigate commercial satellite-based systems to develop an autonomous battlefield personal communications capability. This will include development of a UAV-based system and universal handsets. The current strategy is to work with industry toward developing cooperative research and development agreements.

6.4.9 On-the-Move Antenna

This program will develop a wideband communications on-the-move antenna to support RAP HCTR communications. The antenna will be capable of operating in line-of-sight mode and via an airborne relay. Phased-array antenna technology is being pursued because these antennas are generally lower in profile and more agile than reflectors. There are, however, technical limitations that impact their effectiveness, particularly at low and varying look angles. The RAP antenna program will address these concerns by developing an on-the-move capability for the Common Ground Station antenna and adapting that technology to support the HCTR.

6.4.10 Radio Access Point (RAP)

RAP is a vehicular-mounted self-contained communications center that contains an ATM switch, an HCTR, an on-the-move antenna, a controlling workstation, and interfacing equipment for narrowband tactical systems, to include SINCGARS, EPLRS, NTDR, and the MSE Mobile Subscriber Radio Terminal (MSRT). RAP allows mobile narrowband tactical users to access wide bandwidth networks for voice, data, and video communications.

RAP will seamlessly extend wideband trunks from the tactical point-to-point backbone to lower echelons with support for integrated voice, data, and video access to/from users located on mobile platforms or foot-mobile. A phased approach of developing and demonstrating a RAP capability will be used. It will involve developing, acquiring and integrating the required interfaces, protocols, and software, as well as assembling the system hardware.

The specification phase will develop a high-level system documentation/specification with detailed RAP functional and performance specifications. A laboratory RAP prototype phase (RAP V1) will demonstrate connectivity in a static, laboratory environment. The data rate of the wideband trunk will be a maximum of T1. During RAP V2, a mobile RAP host will be demonstrated in a laboratory environment, using mobile IP with low to medium (2.4 kbps to 56 kbps) data-rate channels. A static RAP field demonstration will incorporate a static version of the HCTR radio provided by the HCTR program. Finally, communications on-the-move will be demonstrated in 1999 using a mobile RAP.

THIS PAGE INTENTIONALLY LEFT BLANK

7. ACQUISITION STRATEGY

7.1 Background

On 30 January 1996, the AAE and VCSA approved Version 4.0 of the ATA. Enforcement of standards contained in the ATA will be critical to ensure interoperability among independently developed programs and systems. All PMs must certify compliance with the ATA to the Milestone Decision Authority (PEO C3S) prior to formal release of draft and final RFPs for any experimental or modernization systems that are part of or require interface with ABCS. Successful application of standards and demonstrated interoperability will be elements considered prior to approving progression to the next phase of system acquisition.

The ATA is largely based on commercial standards. In addition, the use of COTS technology—including commercial standards for computer hardware and software—will accelerate the acquisition process. Standardizing interfaces and replacing military standards with commercial standards will move toward obtaining needed bandwidth and the latest technological capability at industry competitive prices. This will also allow a degree of closure on the rapid pace of technology expansion, given the time span of a normal DoD acquisition.

Since commercial standards are not normally employed in military tactical command and control systems, a major part of the ADO streamlining strategy is focused on incrementally developing requirements definitions through a series of BLWEs and AWEs. Under standard acquisition procedures, the equipping of the brigade-sized EXFOR supporting the TF XXI AWE would have required a high-level acquisition decision; the use of production funding; and long, detailed acquisition competitions. Since the field experiments are being used to define and refine digitization requirements for the entire Army, the use of RDTE funding and a lower-level decision authority was approved for obtaining the necessary equipment and software.

As most tactical and combat vehicles in the Army have no computer or position locating system, the first step in the strategy is to acquire equipment to be added—or *appliqued*—to those platforms. Four different categories of appliques (commercial, ruggedized, militarized, and dismounted) provide the range of ruggedness and portability needed to test how much the Army can incorporate commercial standards in equipment to be used under field conditions.

TRW was the contractor chosen for the first phase acquisition contract (*Force XXI Battle Command, Brigade-and-Below* (*FBCB2*)). TRW is also responsible for developing the software required to provide situation awareness and command and control capabilities.

The applique will be used in the BLWEs and AWEs on the majority of the platforms normally located within the brigade maneuver area, with the following caveats:

- In early experiments at brigade-and-below levels, appliques and ATCCS terminals will both be mounted on C2, intelligence, and CSS command post vehicles. Once ATCCS systems are capable of porting FBCB2 software for later experiments, the then-redundant appliques will be removed.

- Platforms with embedded command and control capabilities—like the M1A2 Abrams—will upgrade their systems and migrate their current C2 software to the FBCB2 software.

- Some legacy platforms will never be fitted with an embedded digital capability. They will always require appliques in order to be integrated into digitized networks.

7.1.1 Applique Description

First-generation applique equipment will consist of:

- Appropriate category of applique hardware.

- FBCB2 software.

- Position/navigation capability.

- SINCGARS and/or EPLRS radio integration.

- BCIS integration (not included in all platform packages).

Additional software modules will provide an interface with embedded systems on the M1A2 Abrams, AH-64D Longbow Apache, and OH-58D Kiowa Warrior. Selected platforms from the Marine Corps and Air Force will also require appliques, based on the degree and scope of their participation in each experiment.

The initial set of appliques will be used primarily for situational awareness and operational control. All similar systems will not receive the same applique. User requirements will dictate which systems within each tactical organization will be appliqued and the degree of ruggedness required, based on the tactical employment profile of each element. Since the cost of the applique rises commensurate with its degree of ruggedness, that robustness must be matched to mission requirements, but not overmatched in terms of expensive and unnecessary capability.

Applique solutions may not be practical on all platforms. Other solutions will be identified for those platforms in which space, weight, power, electrical interference, or human interface restrictions are encountered, or in cases where the applique may restrict mission capability.

The four applique hardware categories are:

- **Version 1 (V1):** a COTS hardware configuration of computer hardware and peripheral items used when an installation kit can provide all shock and environmental protection necessary to meet mission requirements. The COTS approach permits relatively inexpensive upgrades of processing and display capabilities. In TF XXI, V1's are primarily used in tactical wheeled vehicles or other vehicles where the ability to operate on-the-move (OTM) is not critical.

- **Version 2 (V2):** a more *ruggedized* hardware configuration used when required shock and environmental protection can be provided externally to the equipment by the installation kit or *holster*, and there is an operational requirement to operate the applique primarily OTM. In TF XXI, V2's are used in most C2 vehicles and in other track and wheeled vehicles which must have an OTM capability and need a higher degree of ruggedness than the V1 version.

- **Version 3 (V3):** a *militarized* configuration used when required shock and environmental protection must be integrated into the hardware itself, due to equipment mission profiles and/or shock/recoil from weapons firing. The installation kit provides only mount and platform integration. In TF XXI, V3's are used in selected platforms to compare their performance to V2's mounted in similar vehicles and units.

- **DSSU:** a small, Litton Lightweight Computer used to integrate dismounted soldiers into the digital battlespace. The DSS/Ancillary Device will operate in three configurations: one providing a limited off-vehicle remote capability from a platform-mounted V3 unit; one serving as a stand alone soldier-transported unit for dismounted infantry; and the third as a position navigation device, primarily for CSS vehicles.

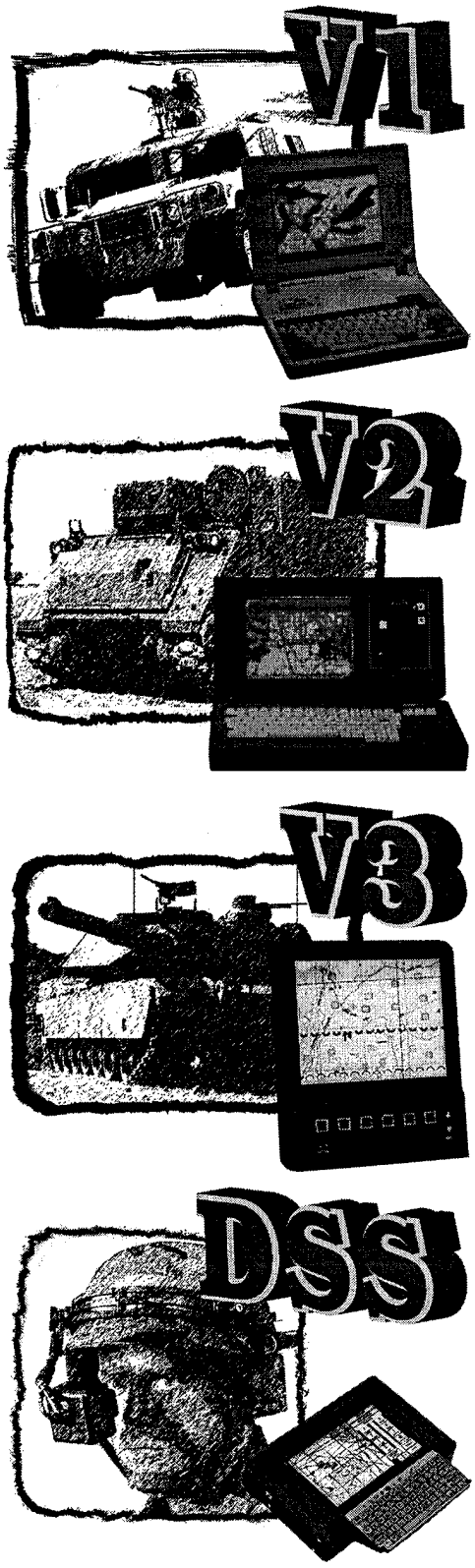


Figure 7-1 Current Appliques

7.1.2 Applique Contractual Requirements

The basic contract provides software, hardware, and systems support to equip a modernized brigade task force organization and its associated divisional support elements (e.g., artillery, engineer, air defense), as well as accommodate data inputs from higher command echelons. The FBCB2 contract also contains an option to procure additional hardware, make software changes, and provide system support needed to conduct follow-on experimentation and required test and evaluation (T&E) of the FBCB2 system prior to a Milestone (MS) III decision.

Specific FBCB2 contract tasks include:

- Developing FBCB2 software.
- Acquiring four types of computer systems (V1, V2, V3, and DSSU).
- Designing and producing installation kits needed to mount the computers on representative Army, Marine Corps, and Air Force weapons systems and C2 platforms.
- Providing contract logistics support (CLS) for FBCB2 hardware and software.
- Creating ICDs with recommended engineering changes needed to install either applique hardware or FBCB2 software in embedded weapons systems.
- Providing the means to technically manage the *Tactical Internet* communications infrastructure.

7.1.2.1 Applique Software

In addition to the applique hardware, the contractor is providing a common FBCB2 system and support software suite. The software suite contains the functionality provided by the C2 portion of the M1A2 IVIS and prototype B2C2 software. The FBCB2 software meets the open system standards described in the ATA, while incorporating and re–using existing government and commercial software to the maximum extent practical. It is also forward-compatible with the mainstream of commercial hardware and software developments to allow ease of new technology insertion in the future. The modularity of FBCB2 software is such that specific modules can be incorporated into embedded weapons systems/platform capabilities, as appropriate.

7.1.2.2 Applique Interfaces

The applique will be connected to several external devices which are installed in the host platform or provided separately. The host platform PM is responsible for planning and programming for these interfaces. They include communications devices, radios, position/location sensors, and on-board platform sensors. The platform PM is also responsible for drilling the holes for mounting the applique set on the host platform.

7.2 Technical Approach

The approach adopted by the ADO involves two basic means for digitizing platform types:

- Installing applique systems on non-digitized platforms.
- Embedding FBCB2 software modules into digitized subsystems to support evolutionary C2 functionality and ensure interoperability with other digitized systems.

7.3 Acquisition Approach

The acquisition approach will be event-driven, featuring a high degree of acquisition streamlining which—from a programmatic standpoint—requires rapid procurement and efficient use of existing funding lines. Acquisition streamlining is necessary to ensure that information technologies can be acquired and fielded before they become obsolete.

The acquisition program is divided into three phases as illustrated in Figure 7-2.

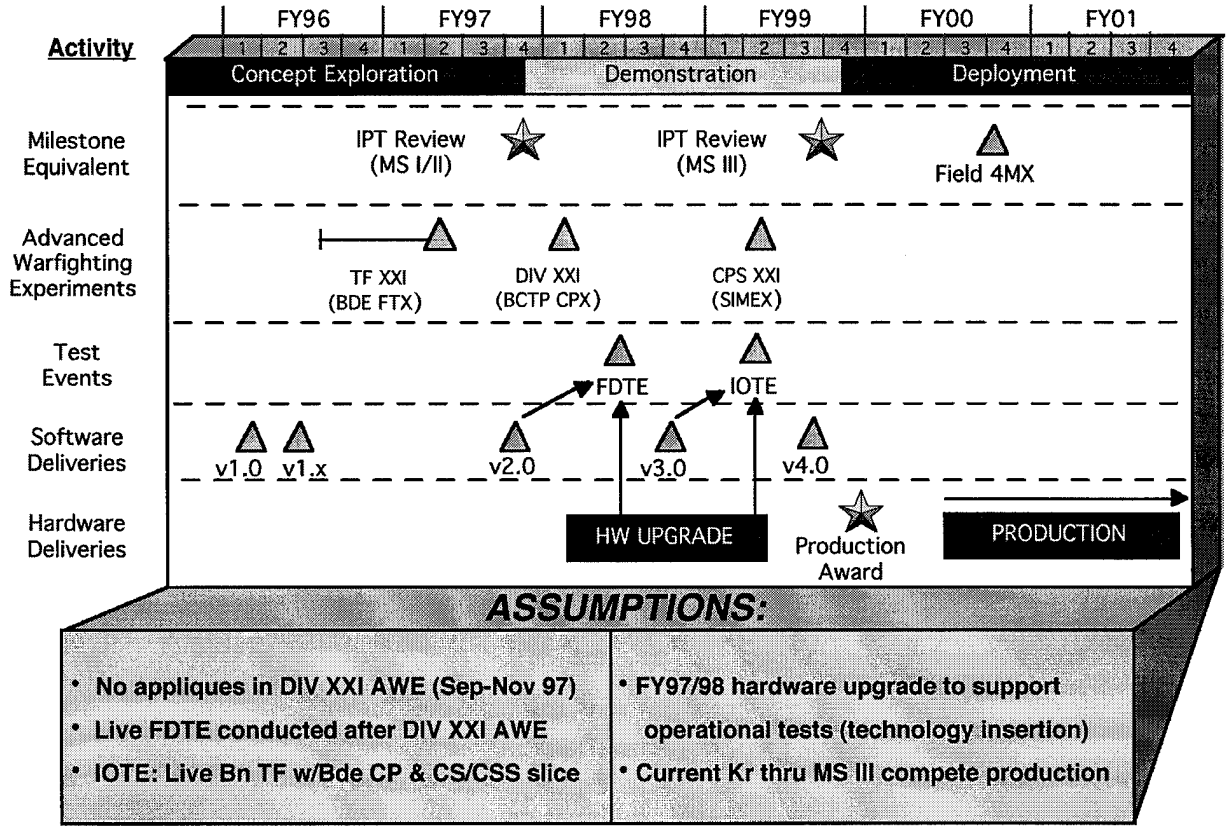


Figure 7-2 Program Milestones

7.3.1 Phase 1: Concept Exploration (FY94-97)

The Concept Exploration Phase began with initial program planning and the definition of a technical architecture. Operational and system architectures are being defined to support digitization of a heavy brigade with attached light forces. These units—a tank battalion; mechanized infantry battalion; light infantry battalion task force; and CS/CSS platoon, company and battalion slices from division assets—have been designated as the EXFOR for the TF XXI AWE. The EXFOR is being built around units of the recently-reflagged 4th Mechanized Infantry Division at Ft Hood, Texas, and will begin experiments following receipt of enhanced digital communications and automated command and control systems in June 1996.

Experimental scope will expand upward from squad/platoon levels in a gradual building block approach, culminating in a full Task Force experiment at the National Training Center (NTC) in February 1997. Following a simulation exercise (SIMEX) in September 1997, a Division XXI AWE will be conducted by the EXFOR Division in November 1997. It will be a Battle Command Training Program (BCTP)-type command post exercise (CPX), with the division's digitized brigade-level tactical operations centers (TOCs) interfacing with the division tactical C2 nodes in a constructive AWE. Only the 1st Brigade's TF XXI TOCs will deploy down to battalion level.

Phase 1 will terminate with a Milestone I/II decision.

7.3.2 Phase 2: Demonstration (FY97-99)

Once a full analysis of the digitized hardware and software performance is completed and an in-progress review (IPR) grants approval to move to the next phase, elements of the EXFOR will be upgraded with improved applique systems. Following an additional train-up period, an FDTE will then take place in FY98 to validate and verify changes made to TTP, hardware, and software. The FDTE will be conducted by elements of TF XXI to conserve resources and reduce train-up/reconfiguration time.

A follow-on Initial Operational Test and Evaluation (IOTE) will be conducted in FY99 to confirm that Critical Operational Issues and Criteria (COIC) have been met. At the conclusion of the IOTE, the mature digital systems are expected to provide a *go-to-war* capability. This phase will terminate with a MS III decision, currently scheduled for FY99.

7.3.3 Phase 3: Deployment (FY00-TBD)

The MS III review will trigger the production contract. It will be competitively awarded and contain several options structured to meet normal 12-month delivery periods for expeditious fielding to Force Package One (FP-1) units. Many embedded systems will be fielded during this period, but appliques will still be needed to support non-digitized legacy equipment—such as the M1A1 tank—and platforms for which no embedded digital capability is planned. Units with older appliques will also be refitted with upgraded versions.

7.4 Funding

Funding efforts are integrated using the Digitization MDEP oversight process. The Director, ADO, maintains control over a portion of the PM's funds until the PM provides a suitable plan that demonstrates adherence to digitization standards and the ATA. The ADO ensures the MDEP funding requirements are programmed, budgeted, and executed in a manner consistent with established Army priorities. The ADO coordinates the MDEP with the ARSTAF; MACOMs; and PEOs/PMs, who must inform the ADO prior to making resource allocation adjustments. Annually, they make recommended adjustments to the MDEP to meet the changing requirements of the Army digitization effort. Results are briefed to the AAE and VCSA.

The MDEP includes funding for various research and development PEs and SSNs related to digitization. Due to the importance of the Operations and Maintenance (O&M) funded activities related to digitization, O&M funding is also included (under *Joint Venture* Experimentation). Additional hardware and software requirements are expected to emerge during the experimentation process. As these additional needs are validated, the funding profile will be adjusted IAW competing priorities.

The ADO will also periodically conduct technical and program execution reviews. Release of program funding contained in the digitization MDEP will be contingent on completing these reviews. PEOs/PMs will provide copies of status reports to the ADO in the same format and frequency as required by their higher headquarters.

7.5 Evaluation and Follow-on Requirements Development

During the initial phase, emerging requirements and technology growth will be assessed to ensure congruence. It can be assumed that the functionality required of the software and hardware—both in appliques and in embedded systems—will grow as user requirements become more refined. The increase in required functionality and industry's capability to provide it will be assessed at each phase of the program.

Since appliques will be installed in some platforms that have other digital systems, FBCB2 software will have to be integrated with those systems. In the initial phase, the contractor will define and document these interfaces and size the FBCB2 software's processing and memory requirements to accommodate these potential interfaces in the future.

7.6 Operational Assessments

Operational assessments will be provided as part of the TRADOC Battle Lab experimentation process and heavily emphasized during the AWEs. Information will be gathered regarding the feasibility, suitability, functionality, reliability, maintainability, and MANPRINT issues associated with the digitized systems. Maximum use of government-validated models and simulations are planned to determine the significant unknowns. Frequent user experimentation opportunities leading to the TF XXI exercise should provide ample data to reduce the scope of follow-on operational and technical tests. Results from such experimentation will provide much of the data required for formal materiel release following Phase 2 completion.

Applique hardware will only be procured for experimental or evaluation purposes and will not be fielded to units other than those units participating in the experiments and evaluations. Following successful completion of the FDTE and IOTE, a full materiel release must be obtained for subsequent fielding and operational use. As embedded C2 systems are modified, they will be evaluated as part of the normal product improvement process.

7.7 Logistics

As the prime contractor, TRW is responsible for defining, designing, refining, and providing CLS for the applique hardware and FBCB2 software—to include spares, repair/replacement, and training—throughout the Concept Exploration and Demonstration Phases. Conversion to organic support as part of the individual platforms' integrated logistics support (ILS) programs will occur during the Demonstration Phase in preparation for the Deployment Phase. For embedded systems, logistics support will use the approach applied to the host platform.

7.8 Trade-Offs

The applique user requirements as stated in the SOW were carefully evaluated to determine which can be supported by current technology. During Phase 1 and prior to Phase 2, emerging requirements and technology growth will again be assessed and evaluated to ensure congruence. Efforts have been made to keep changes in user requirements to a minimum during Phase 1 by prioritizing the functionality required of the applique software and digital hardware and establishing a *good idea cutoff date* to increase the probability of initial success. As Phase 2 is entered, advancements in technology should support the incorporation of additional requirements as they are developed and validated. After the IOTE, a determination should be made as to the cost effectiveness of incorporating additional functionality in the Phase 3 contract.

Integration of applique software with individual platform control systems (e.g., laser rangefinders and hull-turret azimuth indicators) is an ultimate goal of the applique effort. Phase 2 will include preliminary design and sizing provisions to facilitate subsequent efforts toward this goal. The contractor shall be responsible—in conjunction with platform PMs—for ensuring these potential interfaces are defined and documented.

7.9 Sources of Competition

The sources for these acquisitions are those industrial teams consisting of commercial computer manufacturers, software developers, and system integrators who have the ability to satisfy the requirements of the SOW. The Phase 1 contract was awarded to the offeror who was deemed to submit the proposal with the *best value* to the government. It is not practical to set aside this acquisition for small business because of the magnitude and diversity of both hardware and software needs and the extensive manufacturing and system integration efforts required.

Although there will be no set aside for small or small disadvantaged businesses, all required clauses will be included IAW Federal Acquisition Regulation (FAR) 19.702. Subcontracting to small disadvantaged businesses will be a contract requirement, with all required clauses included in the solicitation and contract.

Full and open competition will be the basis for all contract awards. The Government awarded the initial contract to one contractor team at the conclusion of a formal source selection process. This contract included system engineering, software development and integration, hardware, and all support necessary to support the TF XXI AWE and the follow-on FDTE and IOTE. All three experiments/evaluations will serve to provide essential information leading to a MS III decision and a new contract to equip FP-1 units. The emphasis of this approach is on system development and experimentation to determine the requirements for a subsequent production contract to support fielding digital capability for FP-1 and other units over a seven year period. The MS III contract will also be an open solicitation and will be awarded at the conclusion of a formal selection process. Component break-out does not apply to this program since none of the applique components are expected to cost more than one million dollars.

7.10 Risks

7.10.1 Technical Risks.

Adequate NDI hardware and open system architectures already exist in the commercial marketplace. There was no requirement in the initial solicitation that could not be provided by current commercial industrial capability. The challenge and risks of this program center on the ability to *ruggedize* the products, integrate them, and successfully install and operate them on a wide range of military platform types in varied operational environments. Risk was diminished by minimizing and prioritizing Phase 1 technical requirements, and by requiring the contractor to maintain the equipment during Phase 1 while also serving as the total system integrator.

As technical requirements expand during the experiments, they will be included in the contract option for Phase 2, to be awarded in the 1997 timeframe. Because of the expected continued growth in the micro-electronics and computer industries, any expanded requirement for Phase 2 will be kept within the industry's capability and is considered low risk.

7.10.2 Programmatic Risks.

A major consideration in the applique acquisition strategy is to ensure adequate competition for future acquisition. The overall acquisition strategy is for an open architecture which allows for maximum competition within the commercial market. Opening competition in Phase 3 will provide added programmatic risk, but is offset by the added value expected to be obtained through improved technology and competitive procurement for the rest of the applique acquisition. Added programmatic risks result from limited knowledge of various platform operating systems; potential problems associated with additional functionality; risks associated with other subsystems; and the potential need to redesign installation kits in Phase 2.

Selecting a single contractor in Phase 1 for only those quantities of appliques required to support the TF XXI AWE, FDTE, and IOTE will also minimize the effort for RFP preparation, subsequent evaluation, and time to award since the areas of logistics, training, test, and cost can be minimized to cover only the limited scope required. Sufficient time will exist to prepare the Phase 2 acquisition contract option during FY97 for release and award in early FY98. This longer lead time

will allow detailed guidance to be developed for logistics, testing, training, and clarification of production quantities for inclusion in the second contract option.

7.10.3 Cost Risks.

Cost risks for awarding a system integration contract to a single contractor were considered moderate because of the immaturity of Government Furnished Information (GFI) application software; the lack of installation kit definition; the limited information concerning platform operational systems; and the unknowns associated with total system responsibility on the part of the contractor. However, cost risks were reduced through the competitive approach. Phase 1 cost reductions were attained through an open, competitive solicitation for the system integration services and a basic quantity of items to support the planned experiments and evaluations. During Phase 1, knowledge of a follow-on competitive contract award for the post-MS III production quantity will provide incentive for the incumbent contractor to minimize overall cost and incorporate cost savings into the Phase 2 Option. An optional per-item repair contractor maintenance plan can be competed among military depots or other contractors as a potential for additional cost savings during the Phase 2 effort.

8. ASSESSMENT STRATEGY

8.1 Overview

Assessment of warfighting capability for forces equipped with digitization technologies will be based primarily on timely and cost-effective evaluation exercises such as the series of planned AWEs. Validation will also include the implementation of training programs and strategies; results from related operational and developmental tests; and the outcomes of modeling and simulation (M/S) efforts.

The ability to capitalize on opportunities for early testing, experimentation, and simulation in the Battle Lab environment will result in the early identification of problems and required solutions. Army analytic, test, and evaluation communities will be involved in assessing the effectiveness of technologies, doctrine, procedures, and force structures throughout the process. Operational Performance Objectives (OPO), Measures of Effectiveness (MOE), and Measures of Performance (MOP) are established to assess specific changes and track their effect over time. These measures focus on increases in force lethality, survivability, and tempo.

The assessment strategy is guided by the *Experimentation Master Plan (EXMP)* and structured around a *rolling baseline* concept which links the efforts leading up to implementation of Force XXI. These include the primary simulation efforts (live, virtual, and constructive modeling), ACTDs, ATDs, and supporting efforts of combat and materiel developers. As the Army moves toward Force XXI, the *rolling baseline* concept can provide an assessment status of current capabilities at any point in time. It also documents trends of improved force effectiveness to support decisions on implementing concepts and systems, including DTLOMS and TTP.

The *rolling baseline* moves away from a single event-oriented *success/failure* philosophy. It uses data from relevant preceding experiments and exercises as the baseline for the next experiment or exercise. The assumption is that there should be a trend in improved force effectiveness over time as new system technologies, doctrine, procedures, and force structures are introduced. Since experiments will focus on different employment concepts, the idea of showing a trend over time provides a means to assess which concepts have the greatest potential. M/S are key to screening new concepts and establishing new and revised goals for each new cycle of anticipated improvements. Developing stable scenarios—especially for the larger constructive simulations—will facilitate study responsiveness and the ability to compare the effects of new capabilities to those in the baseline.

This cyclic process supports the ADO's evaluation of the value-added by digitization, while minimizing the need for large scale, costly field experiments and exercises. AEPG will be the forum to facilitate the close coordination and cooperation needed among the M/S, system developer, evaluation, and test communities.

8.2 Experimentation, Testing, and Evaluation

In executing the *Joint Venture Campaign Plan*, the Army will conduct a series of AWEs and BLWEs to demonstrate improvements in force effectiveness as a result of fielding digital information technologies and implementing changes in organizational designs and TTP. These experiments will be designed to provide insights and yield data to address operational force effectiveness and system level performance issues.

Appliques and modernization equipment will be examined in these experiments to establish an early understanding of their warfighting potential. Each experiment will build upon the results of previous experiments, creating the *rolling baseline* to measure increases in force effectiveness.

Opportunities for data collection will also occur in the course of fielding digitization equipment to the EXFOR. For example, during scheduled individual and crew training on the operation and use of the equipment, data will be obtained on both system performance and suitability. By taking advantage of these opportunities, the need and/or scope of separate operational and technical tests should be diminished.

In general, there will be five classes of experimentation and testing conducted to support the development and evaluation processes:

- DIL certification and preliminary examination of prototype hardware and software to verify ability to perform critical functions and meet interoperability requirements.

- Virtual, constructive, or live BLWEs to examine new equipment, processes, and force design issues, providing significant opportunities for rigorous data collection to satisfy evaluation requirements.

- AWEs conducted in a tactically rigorous environment to confirm experimental hypotheses regarding increases in warfighting capability while minimizing interference with training, realism, and other objectives.

- Technical tests (TTs) conducted after successful DIL certification and in parallel /coordination with BLWEs and operational tests. TTs take place in stressful and controlled environments and confirm that critical technical parameters and contractual specifications have been met.

- Operational tests (OTs) conducted to obtain data on total system performance when employed by representative soldiers in an operational environment. OTs will be conducted as necessary to fill *data voids* in order to provide credible operational assessments for subsequent procurement and fielding decisions.

8.2.1 Advanced Technology Demonstrations (ATDs) and Advanced Concept Technology Demonstrations (ACTDs)

ATDs seek to mature advanced technology and demonstrate its potential for enhanced military operational capability and/or cost-effectiveness. They are complex and often resource-intensive; involve operators/users from planning through final documentation; are tested in a real and/or synthetic operational environment; are typically completed in five years or less; and are cost, schedule, and performance baselined.

Before technology can make the stepped transition from concept exploration to development, it must meet or exceed exit criteria mutually agreed by the user and/or Battle Lab and the ATD manager. This helps the user develop more informed requirements and assists the materiel developer in reducing risk prior to entering a formal system development phase.

ACTDs are also jointly planned by the warfighter and acquisition communities, with sponsorship by a Unified Command strongly desired. ACTDs seek to have the user evaluate the military utility of the concept before committing to future acquisition and developing corresponding concepts of operation and doctrine that optimize the new capability.

8.2.2 Advanced Warfighting Experiments (AWEs) and Other Digitization-Related Experiments

Through an iterative series of modeling, simulations, and AWEs, *Joint Venture* focuses on providing early digitized capabilities; organizational redesign; and new TTP. Two 1994 events—Desert Hammer and Desert Capture III—became the baseline for follow-on AWEs. Five AWEs conducted in 1995 have been fundamental in helping to determine the design of future units: Atlantic Resolve, Theater Missile Defense, Prairie Warrior/Mobile Strike Force, Focused Dispatch, and Warrior Focus. These AWEs revealed much about the capabilities of advanced technologies and how best to employ them to meet the operational challenges of the 21st Century.

Sufficient train-up time precedes each AWE to allow participating units to become proficient in the fielded digital capability and refine their TTP. This time also provides data collection opportunities for independent agencies to gather empirical data for subsequent analysis to determine the value-added from insertion of battle command digital technologies. Each experiment is an iterative process to establish a *rolling baseline* for subsequent experiments.

Experimentation and testing of digital information technology will be designed to determine adequacy of requirements; to identify the best use of new capabilities; and to collect data necessary to provide credible evaluations in support of procurement decisions. Continuous evaluation through constructive, virtual, and live experiments and separate operational and technical testing will verify equipment progress toward meeting mission needs and performance objectives.

8.2.2.1 Atlantic Resolve

Atlantic Resolve—formerly called Reforger—was conducted by United States Army Europe (USAREUR) in November 1994 as a large-scale, joint and combined deployment and theater campaign. It provided valuable insights about linking disparate constructive, virtual, and live simulations in a common synthetic theater of war (STOW). As the STOW concept matures, it will become an integral component of the Division XXI and Corps XXI AWEs.

8.2.2.2 Prairie Warrior/Mobile Strike Force (PW/MSF)

The PW/MSF 95 AWE was conducted in May 1995 by the TRADOC Battle Command Battle Lab at Ft. Leavenworth, Kansas, to explore force design for Force XXI. The AWE used officers from the Command and General Staff College commanding and controlling a simulated 21st Century division. The MSF was used to examine issues associated with a new land combat force structure derived from TRADOC Pamphlet 525-5. The AWE used the constructive Corps Battle Simulation (CBS) to experiment with various new designs and future equipment.

An additional objective was to look at how the division TOC could be reorganized and streamlined around information, and which 21st Century technologies had the greatest impact on this operational construct. No applique hardware or software was available for PW/MSF 95, but the ATCCS family of systems, Terrain Evaluation Module, prototype Phoenix system, Log Anchor Desk, and other technologies were employed. It was observed that the digitized battle staff did not offer significant advantages over the traditional staff structure. However, the limitations of the simulation, student inexperience with the digitized equipment, and the use of immature technologies prevented an examination of warfighting concepts as originally intended.

8.2.2.3 Theater Missile Defense (TMD) AWE

The TMD AWE conducted in May 1995 was a Joint Service exercise that used a combination of live, virtual, and constructive simulations to provide a holistic review of National, Joint, and Army capabilities. The purpose was to evaluate the ability of a cohesive TMD force to counter the enemy across multiple operational phases (pre-attack, attack, and post-attack). The TMD AWE combined attack, active defense, and passive defense operations with a robust C4I system. The effect to be obtained from the combination of forces and C4I was a strategic force that allowed no sanctuary for conventional and unconventional tactical and ballistic missile threat operations. The AWE provided an initial examination of the EAC perspective on issues associated with TMD for the digitization baseline assessment.

TMD used C3 technology insertions from ATDs and ACT II programs such as Common Ground Station; Digital Battlefield Communications; Battlefield Distributed Simulation-Developmental; and Anti-Armor and Ferret Simulations. Applique technology was not available for this AWE. The primary item of interest to the ADO was the application of the integrated TOC structures at brigade and joint task force levels. These TOCs proved the potential of integrated and co-located ATCCS equipment. Lessons learned are expected to be applied during follow-on AWEs.

8.2.2.4 Focused Dispatch AWE

Focused Dispatch was a series of Mounted Battlespace Battle Lab (MBBL)-sponsored experiments conducted from April through August 1995 at Ft. Knox, Kentucky. Constructive, virtual, and live simulations were employed to gain training development and small unit effectiveness insights for digitized forces. A battalion task force organization was used to address the organizational, doctrinal and TTP changes necessary to fully realize the potential offered by digital information and communications connectivity. Focused Dispatch assumed that full connectivity functions were in place, while discrete systems were not assessed for their individual contribution to force effectiveness. Objectives included maximizing information connectivity; determining needed changes in command processes and functions; and adjusting organizational mixes to take advantage of potential digital benefits and improve lethality, survivability, and tempo.

Digital systems at the battalion level included IVIS and the B2C2 communications software to link IVIS, ATCCS, and various non-digitized platforms. Appliques were not available for this AWE, but the prototype B2C2 software offered the same basic functionality. The ADO's primary interest in Focused Dispatch was the development of digitized TTP for the EXFOR's TF XXI mechanized and armor units. In addition, the ADO hoped to gain insights into what functions/displays are most useful during various phases of the operation and what additional functionality/displays are needed that can be made a part of the applique.

8.2.2.5 Warrior Focus AWE

Warrior Focus established a baseline for the digitization of the dismounted soldier in a mixed light-heavy task force with Special Operating Forces (SOF) attached. The AWE was conducted at the Joint Training Readiness Center at Ft. Polk, Louisiana, in November 1995. The Dismounted Battlespace Battle Lab (DBBL) planned to look across all BOSs and concentrate on warfighting benefits to support Force XXI doctrine, equipment and tactics. Warrior Focus experimented with digital technology—similar to the planned capabilities of the dismounted version of the applique—using B2C2 software to link the soldier to the battalion and establish links across the BOSs. Prototype communications and other systems from ATD and ACTD programs were also examined during the experiments, such as DBC, BCIS, Combined Arms Command and Control (CAC2), and the Rapid Force Projection Initiative. The ADO's interest in Warrior Focus is in several areas directly supporting the TF XXI AWE, such as development of digital TTP for the EXFOR's light and mechanized infantry units; insights into the functioning and functionality of the DSSU; and a preliminary basis of issue plan for digital equipment for the dismounted soldier.

8.2.2.6 Prairie Warrior 96

Planning has just begun for Prairie Warrior 96. Prairie Warrior will exercise the proposed Force XXI Division design, with elements from the EXFOR serving as players. The ADO's interest is in TOC development and design, integration of the ATCCS systems, and the maturity of MCS/P system development. Also of interest is the identification of simulation improvements to support the evaluation of digitization during the Division XXI AWE.

8.2.2.7 Joint Warfighting Interoperability Demonstrations (JWIDs)

JWID 95 was one in a continuing series of Joint Staff-sponsored demonstrations oriented on interoperability and joint operations objectives that are intended to advance the *C4I for the Warrior* concept. Army demonstrations for JWID 95 are grouped into five areas:

- **Battlespace Management**: providing the Joint Task Force commander the capability to maintain a common picture of the situation with his subordinate components using C4I systems and networks.
- **Communications and Networks**: focusing on *transmission* as opposed to *application.*
- **Distributed Collaborative Planning**: orienting on processes providing real-time, simultaneous interaction among multiple users, using a wide variety of planning tools.
- **Knowledge-based Information Presentation**: demonstrating systems designed to allow the commander to concentrate on *product* rather than *process*, by constructing user-friendly interactive interfaces between the decision maker and the complex collection of automated and manual information resources.
- **Warrior Smart Push/Pull**: advancing the art of obtaining and providing information.

The ADO's interest in the results of JWID 95 is mainly on the viability of the demonstrated technologies for continued development and incorporation into digital communications and networks. These include TMG ISYSCON network management and satellite communications technologies. In addition, connectivity was demonstrated with elements from the United Kingdom.

JWID 96 is in the initial planning stages, with the Army designated as the lead Service. It is expected that there will be significant multinational play in the exercise. Unlike previous JWIDs, JWID 96 is envisioned to be a four-phased experiment. Phase 1 will entail setting up the network and demonstrating its viability; Phase 2 will demonstrate the latest C4I capabilities to the Warfighter; Phase 3 will train the digitized battle staff on selected C4I systems; and Phase 4 will be the C4I Joint Warfighter Exercise. The focus for the ADO will be on assessing digitized links between the joint task force and a division headquarters.

8.2.2.8 Force XXI AWEs

The critical event taking place from June 1996 through February 1997 will be the TF XXI AWE. This will be the first of three major AWEs at brigade, division and corps levels designed to test digitally-based concepts, organizations, and equipment prior to fielding Force XXI. The TF XXI AWE begins with equipment fielding and operator training; progresses through unit train-up and exercises of increasing scope and complexity; and culminates in a brigade-level exercise conducted at the NTC. All AWEs will include varying degrees of participation from the other Services.

The major goals of the AWEs are to:

- Document improvements in survivability, lethality, and operational tempo resulting from the insertion of digitized technology.
- Verify the utility of changes in force structure changes and TTP.
- Provide insights into brigade, division, and corps command and control processes.
- Provide insights into Army/Marine Corps command and control interoperability.
- Develop and refine joint warfighting doctrine.

The *EXMP* prepared by PEO C3S will guide the initial assessment of the applique during the TF XXI AWE. OPTEC and the Army Materiel Systems Analysis Activity (AMSAA)—the Army's independent evaluators—will coordinate their evaluation support through the *EXMP* in conjunction with the ADO, materiel developer, TRADOC, AMC (CECOM), and FORSCOM.

The objectives for the TF XXI AWE are to:

- Develop a tailorable force design capable of conducting combat and peacetime operations as part of a joint and/or multinational force.
- Determine the implications of organizational, technological, and associated TTP enhancements on soldiers and leaders through simultaneous experimentation and technology insertion.
- Determine the appropriate TTP associated with an *Information Age* force.
- Experiment with enhanced battle command capabilities.
- Analyze applique hardware and software with sufficient rigor to make subsequent acquisition recommendations.

TF XXI will allow the Army to examine the effects of digitization at the brigade task force level. The series of scheduled training events will provide slices of information pertinent to the effects that the digital applique will have at various levels of the force. This will be the first full-up look at applique hardware and software. Once the analysis of the TF XXI AWE is completed, it will become the *rolling baseline* for future exercise comparisons.

8.2.2.8.1 Marine Corps Participation in Task Force XXI

During the TF XXI AWE, the Marine Corps Systems Command will simulate a ground-heavy MEU to investigate digital interoperability means at all echelons of the ground combat element. The special purpose Marine Air-Ground Task Force (MAGTF) will include elements of infantry, tank, assault amphibian, and light armored reconnaissance units to cover the widest variety of potential ground platforms. Capabilities to be demonstrated by the Marines in each segment of the program are:

- Command and control at the battalion-and-below levels.
- Combat identification systems.
- Tactical Data Network at Echelons-Below-Battalion (TDN-EBB).

Marine participation in the TF XXI AWE will consist of a series of experiments and evaluations, beginning in June 1996 and ending in February 1997. The following experiments will be designed to measure improvements in unit combat effectiveness as a result of information technology improvements:

- **Light Force Reaction Experiment** (1st Qtr 96) comparison of a platoon with current C2 systems to a platoon outfitted with battalion-and-below command and control/situational awareness (C2/SA) and TDN-EBB systems.
- **Strike Force Raid Experiment** (4th Qtr 96) will be similar to the preceding experiment, but will use an infantry company reinforced with platoons of AAVP-7s, tanks, Light Armored Vehicles (LAVs) and attachments from the battalion weapons company.
- **Rolling Thunder Experiment** will be similar to the above experiments, but will use an infantry battalion reinforced by a light armored reconnaissance company, a platoon of AAVs, and a platoon of tanks.
- **Task Force XXI AWE** (Feb 97) will combine the MEU command element and other units not previously exercised.

All experiments will be structured so that interoperability evaluations with equivalent Army systems can be made. Interoperability with Navy and Air Force systems will also be examined.

8.2.2.8.2 Air Force Participation in Task Force XXI

During TF XXI, Air Force support to the Army will be orchestrated by the Tactical Air Control Party (TACP) at the brigade and maneuver battalion levels. Current plans are to outfit the TACP with a DSSU-based position-navigation device (PND) within the TACPs' tracked and wheeled vehicles. Currently there is no direct digital link between FBCB2 and the Air Force Digital Communication Terminal (DCT). Any information received from an applique will have to be re-entered into the DCT for ground-to-air transmission.

The Air National Guard is testing the use of EPLRS coupled with a Situation Awareness Digital Link (SADL) in fighter aircraft. An Army EPLRS ground station will be provided to serve as a net control station for transmitting situation awareness data to supporting aircraft.

8.2.2.9 Division XXI and Corps XXI AWEs

The Division XXI AWE will feature a division-level BCTP-type CPX exercise in November 1997, preceded by a SIMEX in September 1997. The Division XXI AWE will examine the connectivity within a division and between the division and its corps slices, providing the Army with a first

look at the *Digital Division.* Analyses and lessons learned from Division XXI AWE will then form the *rolling baseline* for a Corps AWE to be tentatively conducted in FY99, with scope and objectives to be determined.

For the Division XXI AWE, the Marine Corps will simulate a balanced MEU by increasing the degree of play for aviation units compared to TF XXI. For the Corps XXI AWE, Marine Corps participation will be determined by the results of the prior AWEs.

8.2.3 Force Development Test and Evaluation (FDTE) and Initial Operational Test and Evaluation (IOTE)

Recent downscoping of the Division XXI and Corps XXI AWEs has significantly reduced the amount of experimentation data that was originally to have been collected. As a result, a full FDTE (FY98) and IOTE (FY99) will be conducted prior to a Milestone III decision on procurement and fielding of the applique systems (see section 7.3.2 for a full description). A Test Integration Working Group (TIWG) chaired by PM Applique is working on scope and funding estimates and the development of a required TEMP. TRADOC will be responsible for revising the FBCB2 ORD and developing the COIC, which will emanate from the results of the TF XXI AWE and other parallel Force XXI initiatives.

8.3 Digital Integrated Lab (DIL) and Interoperability Certification

The DIL is a subordinate element to the CECOM Research, Development and Engineering Center (CERDEC) at Ft. Monmouth, New Jersey. The purpose of the DIL is to evaluate system-to-system, link-to-link, and net-to-net interoperability for all systems which are required to interoperate in the Force XXI AWEs. The DIL develops, maintains, improves, and recommends certification for interoperability between and among C4I and Electronic Warfare (EW) hardware and software. All C3 systems which must interoperate are required to be certified by the DIL prior to participation in AWEs. Systems being developed, systems already fielded, and S&T programs are also encouraged to use the DIL to develop and verify their interoperability.

The DIL is a dynamic, integrated facility that can be rapidly reconfigured to replicate diverse existing and evolving tactical C3I/EW *systems–of–systems* in quasi-battlefield environments. It consists of interconnected distributed laboratories, test beds, battle labs, field sites, contractor testbeds, and simulation facilities, along with on-site technical engineering expertise at each location. This allows comprehensive evaluations of new prototypes, evolutionary system developments, continuous systems sustainment, and systems interoperability through the application of new technologies, tactics, and doctrinal, organizational and operational concepts.

The DIL performs the following four AWE support functions:

- Supports PEO/PM informal experimentation with Force XXI C3I/EW systems.
- Supports informal experimentation with fielded C3I/EW systems and S&T programs.
- Certifies interoperability of C3I/EW systems prior to an AWE.

- Evaluates compliance with ATA standards, procedures, and models.

A sampling of the many systems expected to participate in the DIL certification process are listed in Figure 8-1. Interoperability certification verifies that each combination of different systems and equipment used in the operational environment is interoperable and considers the transmitting and receiving hardware and software; communication/transmission media/devices; associated protocols; and message types.

Advanced Field Artillery Tactical Data System	AFATDS
All Source Analysis System	ASAS
Applique	Applique V1,V2,V3
Army Airborne Command and Control System	A2C2S
Automated Nuclear, Biological, Chemical Information System	ANBACIS
Battle Command Identification System	BCIS
Bradley Stinger Fighting Vehicle–Enhanced	BSFV-E
Command and Control Vehicle	C2V
Dismounted Soldier System Unit	DSSU
Enhanced Position Location Reporting System–VHSIC	EPLRS–VHSIC
Forward Area Air Defense Command, Control and Intelligence	FAADC2I
Lightweight Video Reconnaissance System	LVRS
Maneuver Control System/PHOENIX	MCS/P
Mission Planning and Rehearsal System	MPRS
Mortar Fire Control System	MFCS
Position Location Ground Receiver	PLGR
SINCGARS SIP/INC	SINCGARS SIP/INC

Figure 8-1 DIL Certification Participants (Extract)

In addition to CERDEC facilities at Ft. Monmouth, the DIL provides connectivity via the Army Interoperability Network (AIN) and the Defense Simulation Internet (DSI) to other C3I/EW facilities at Ft. Monmouth, the Battle Labs, the JITC, and other government and contractor facilities. The core of the DIL can be rapidly reconfigured to meet the needs of potential customers and can be electronically extended to the customer's location. The concept of a distributed test is based on the cost effectiveness of being able to use a facility or system via remote access instead of bringing the system or facility to a central location or having another facility or system built at the central location. This distributed architecture normally has three components: a central core; the remote facilities and/or systems; and the communication network that ties it all together. DIL efforts will improve system performance and quality by identifying interoperability issues early in system design and providing the materiel developer with opportunities to modify and adjust the system without major programmatic impacts.

8.4 User Jury Process

A user jury has been established to conduct FBCB2 software assessments to ensure that timely, meaningful feedback is provided to PM Applique. Duplication of work is avoided and efforts are

optimized by incorporating previous *rapid prototyping* lessons learned by other Battle Labs and by making use of contractor testing.

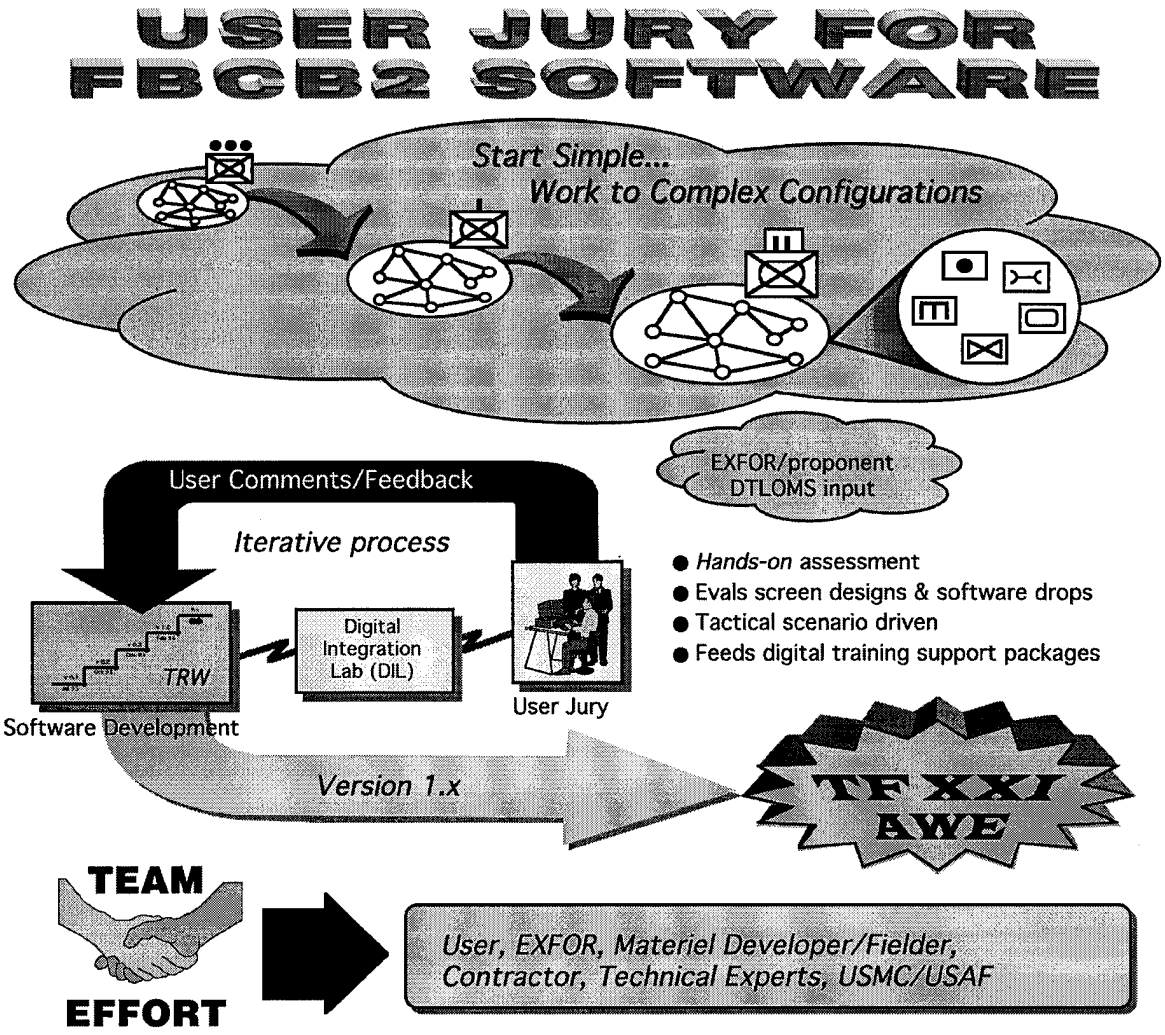


Figure 8-2 User Jury Process

The MBBL is the TRADOC lead for the user jury assessment. The jury is composed of personnel representing each TRADOC school component, plus representatives from the USAF, USMC, and the EXFOR. The exact composition of the group determined by the MBBL Director in coordination with HQ TRADOC, the EXFOR, and BOS proponents. Representatives from PM Applique, ADO, and TRW will be invited to observe the proceedings.

The MBBL will use the assessment process to develop lessons learned from Focused Dispatch to provide TTP for TF XXI. The user jury will convene in conjunction with each software build release; provide critical review and comments; and repeat the process as often as required. Using

the appliques at Ft. Knox, the user jury will link via the AIN to the DIL at CECOM, the EXFOR at Ft. Hood, and to functional proponents for electronic connectivity and rapid contractor feedback.

The user jury process reduces the risk of developing software by re–using previously developed code as a basis for providing new functionality and incremental software deliveries. Feedback from the user jury and system engineering analyses will guide incremental software releases prior to TF XXI. Consequently, TF XXI software will undergo four *user cycles* plus nine months of hands–on experience prior to the TF XXI exercise at the NTC. Assessments will also feed development of digital training support packages for the EXFOR.

8.5 Funding Strategy

AWEs and BLWEs are primarily funded by TRADOC. The ADO views BLWEs and other off-line experiments as stepping stones to the larger AWEs and ultimately to the Force XXI objective. As such, the ADO supports these efforts by assisting in defining the objectives of the various experiments and providing qualified funding for hardware and software necessary to fulfill digitization objectives. Comprehensive funding for AWEs, specific digitization objectives, and DTLOMS development is a coordinated process with the ARSTAF, TRADOC, ASA(RDA), and the ADO working together to identify and resolve funding issues associated with each AWE on a case-by-case basis.

8.6 Modeling and Simulation (M/S)

Models and simulations are used throughout the digitization effort to evaluate operational and technical architectures, alternative technologies, interoperability, and force effectiveness issues. An objective simulation environment is needed to support digitization design, development, training, and experimentation. This objective environment integrates system performance models, constructive models, and virtual simulations through the use of Distributed Interactive Simulation (DIS) in a seamless evaluation environment.

All M/S agencies within the Army have been working together to ensure that M/S is available to support TF XXI and follow-on efforts. Primary agencies include the Army Simulation Strategic Planning Office (DAMO-ZS) as the focal point for M/S on the ARSTAF; the TRADOC Analysis Center (TRAC) as the lead analytic agency for Force XXI; the National Simulation Center and the Simulation, Training and Instrumentation Command (STRICOM) as developers of Army training simulations; and CECOM as the Army agent for C4 modeling. This objective environment integrates system performance models, constructive models, and virtual simulations through the use of common representations. These include system and technology performance, architecture designs, network components established by CECOM, and environmental impacts (e.g., electronic warfare) established by the Test and Evaluation Command (TECOM).

All M/S used to support the ADO assessment of digital communications will be verified and validated by the sponsoring/developing organization and accredited by the using organization. This verification and validation requirement includes combinations of separate models, such as a digital radio model interacting with simulators in a DIS mode. Data requirements to properly

calibrate the models must be clearly identified by the M/S organization, with the required data collected during live experiments by the test agency.

8.6.1 System and Network Design and Performance

The CAC2 ATD is developing system performance models and simulations to support the design and development of the applique and *Tactical Internet*. The CAC2 ATD provides models and simulations of the following: SINCGARS SIP and EPLRS VHSIC radios; terrain and propagation effects; MIL STD 188-220A; Internet protocols; routers; INCs; direct broadcast and MSE packet networks. These simulations are being used separately and in combination for trade-off studies involving protocols, technologies, and performance parameters.

8.6.2 Force XXI Training and Experimentation

DAMO-ZS, the National Simulation Center, and AMC (CECOM and STRICOM) will coordinate DIS modeling and simulation development efforts to insure that training and experiments supported by DIS have realistic network and system performance representations. Two elements are required: integration of realistic communications and integration of the applique. Integration of SINCGARS and EPLRS radios developed under the CAC2 ATD has been accomplished and was used for the first time during Focused Dispatch to provide realistic communications between the live experiment and virtual *simulation networking* (SIMNET) elements. STRICOM is currently exploring engineering alternatives to integrate the applique into SIMNET in support of the EXFOR train-up period, which begins in June 1996. Once this integration is accomplished, the TRADOC Battle Labs and EXFOR expect to use DIS to explore issues dealing with man-machine interfaces, use of digitally provided information, and concepts of employment.

TRADOC has also identified an approach to integrate the applique into the JANUS model to support EXFOR training. The ADO tasked CECOM and the Battle Command Battle Lab at Ft. Gordon to identify C3 improvements for other Force XXI models and simulations, such as brigade-and-below and corps-and-below simulations needed to support the Division XXI AWE. A Division XXI PAT has also been formed to further define required simulation improvements. Both models require enhancements to C3 representations inside the simulations, as well as an ability to link with SIMNET and actual C4I systems. An interface is also needed to allow the applique to interact directly with these simulations.

8.6.3 Force XXI Force Effectiveness Assessments

CECOM and TRAC are working together to incorporate appropriate characteristics of the CAC2 ATD system performance models into various force-on-force constructive models (CASTFOREM and JANUS). This will enhance the play of C3 systems and subsequent C3 impacts on force effectiveness. Constructive force-on-force models and simulations are key to the *rolling baseline* assessment concept proposed for Force XXI AWEs. This cyclic modeling process supports the ADO's evaluation of the value-added by digitization, while minimizing the need for large scale, costly field experiments and exercises.

8.7 Assessments and Evaluations

In summary, the assessment strategy has the capability to provide an assessment of current capabilities at any time and to document trends of improved force effectiveness. Since the assessments will consider information from all data sources, they will support numerous decision points for materiel programs, to include the Applique. For example, the post-TF XXI assessment will consider and report on *all* initiatives that participate in TF XXI. OPTEC will prepare the abbreviated operational assessments, operational assessments, and test and evaluation reports, while technical evaluations will be prepared by AMSAA in support of subsequent IPRs and materiel decisions.

9. RELATED DIGITIZATION IMPLEMENTATION EFFORTS

9.1 Risk Management

The Army digitization effort involves multiple activities, systems development, and operational organizations working together to achieve digitization goals. As with any effort of this size and complexity, there are undesired events or *risks* which—if they occur—may prevent or impede the attainment of those goals. Prudent management requires that a process be established to identify and manage these risks. The ADO *Risk Management Master Plan (RMMP)* provides policy and guidance regarding risk management; describes the risk management process; defines an organizational structure to manage risk; and proposes an initial description of suggested broad risk areas perceived to exist with digitization.

Risk management is envisioned as a seamless process beginning with individual programs and projects and continuing to the highest levels of system and systems integration required by Force XXI. Individual programs and projects that are components of the overall digitization and Force XXI effort are expected to have individual risk management plans in accordance with acquisition directives. The *RMMP* is an overarching master plan focusing on the critical digitization risks.

The *RMMP* has both far and near–term focus. In the far–term, it orients on the risks associated with the implementation of the TA and the acquisition and assimilation of *Information Age* capabilities into Force XXI. The near–term focal point of risk management is on the development of key digitization technologies (e.g., FBCB2 software, *Tactical Internet*, and NTDR) and the successful demonstration of their capabilities in the AWEs.

The *RMMP* is a living document and will be updated by the ADO after each AWE.

9.2 Experimental Force Fielding Plan

The 4th Mechanized Infantry Division (formerly 2nd Armored Division) stationed at Fort Hood, Texas, was designated as the EXFOR. The following criteria were used in determining the recommended equipment list for the EXFOR:

- The EXFOR will include primarily only those 4ID(M) units at Fort Hood.
- The Division (–) will be provided with force modernization equipment, not just the brigade participating in the TF XXI AWE.
- New equipment training (NET) and fielding of modernization systems will be completed by June 1996, permitting nine months for unit combat proficiency training.
- Equipment fielding priority will be digitized equipment followed by the most modern systems available, without delaying any existing First Unit Equipped (FUE) date.
- Use of prototypes or surrogates will be considered where applicable and supportable.

- The EXFOR will retain all fielded modernized systems upon completion of the AWEs.
- The *Department of the Army Master Priority List (DAMPL)* will not be altered, but fielding of EXFOR equipment would be accelerated in an out-of-*DAMPL* sequence.

Exceptions to the June 1996 deadline for fielding will be approved by the EXFOR General Officer Working Group (GOWG), chaired by TRADOC with HQDA participation.

Figure 9-1 reflects the current schedule for providing prototype or production systems to the EXFOR or supporting units. For production systems, the schedule reflects complete fielding, not just the system quantities required for experimentation.

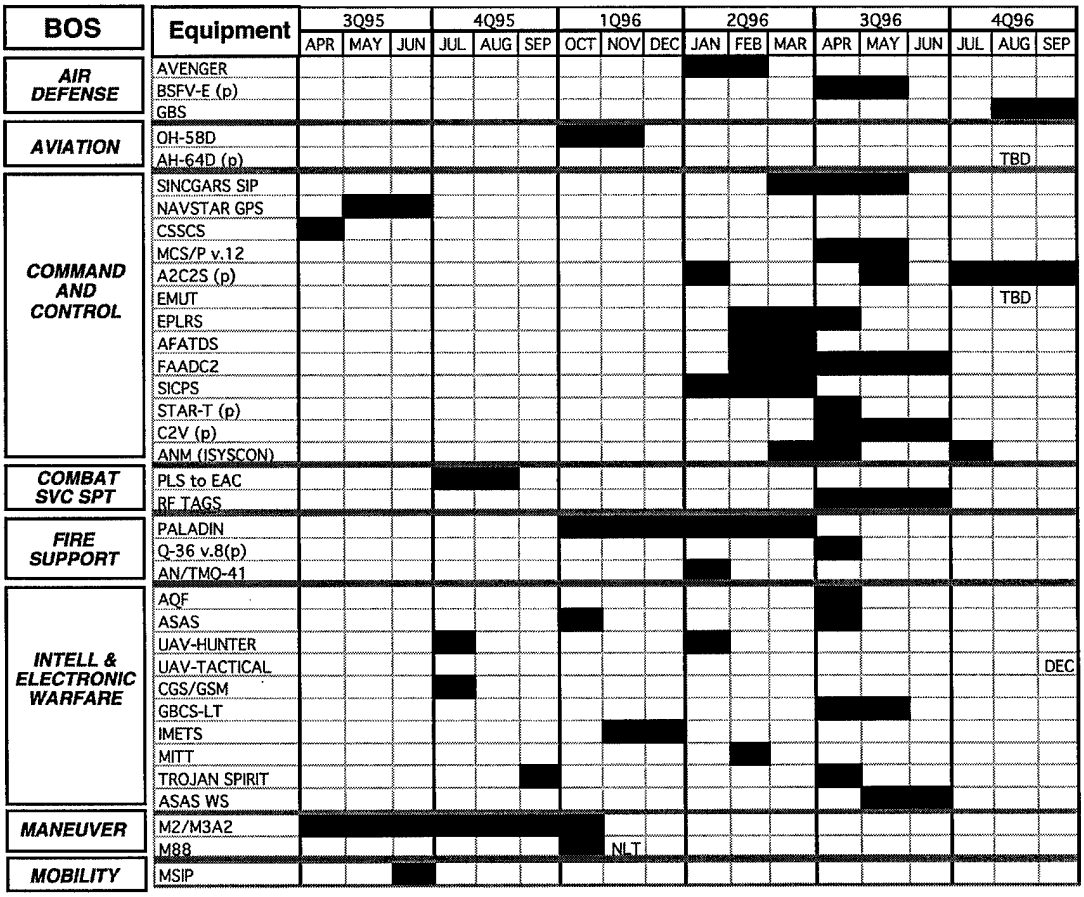


Figure 9-1 EXFOR Fielding Summary as of 1 Feb 96

The Army will not procure an additional brigade or division set of equipment for use solely by the EXFOR. To field the most modernized systems to the EXFOR, the original FUE unit for many digital platforms has changed to 4ID(M). In some cases, 4ID(M) was not originally scheduled to

receive an item of required equipment and higher priority units were displaced on the fielding schedule.

Once modernized, no unit will be *de-modernized.* Additionally, items requested for TF XXI that normally would not be issued to a brigade will be fielded to a divisional or corps supporting unit. FORSCOM, III Corps, and the EXFOR must task organize their assets to ensure that these units participate in appropriate AWEs.

Basis of Issue Plans (BOIPs) on approved requirements will not be violated. If additional items of equipment are required that would exceed BOIP requirements, then FORSCOM must redistribute from within existing assets.

9.3 Security

This section delineates the strategy for ensuring that acceptable information security is provided for Force XXI and all digitization actions leading to Force XXI. It does not address other facets of security (such as physical security and operational security) which are directed by other Army elements.

9.3.1 The Security Challenge

Infusion of *Information Age* technology into the Force XXI battlespace has increased the vulnerabilities of our information systems and created a more complex scenario for protecting the information distributed throughout that battlespace. Expansion of automation devices in weapons systems and command and control; the increased networking of those devices for improved horizontal and vertical connectivity; and the tremendous increase in supporting data communications have brought about a commensurate increase in protection requirements.

Information security risks have increased exponentially through the sheer numbers of information access devices planned for the Force XXI battlefield. Enemy possession of these devices or unimpeded access to the digital data could inflict severe damage on friendly forces. Such risks must be assessed and properly eliminated, mitigated, or accepted in the evolution to the digital battlespace. Protection must be provided to the information being processed/transported—to avoid compromise, exploitation, or corruption—and to the information systems themselves, to avoid information denial.

The Army's challenge is to identify the vulnerabilities of the digital infrastructure; assess the corresponding threat/risk; and manage information system development and investment strategies to provide C4 protection at acceptable risk. During any operation, certain near-term information security risks may have to be accepted to capitalize on the technical advantages of today's weapons and battle command systems.

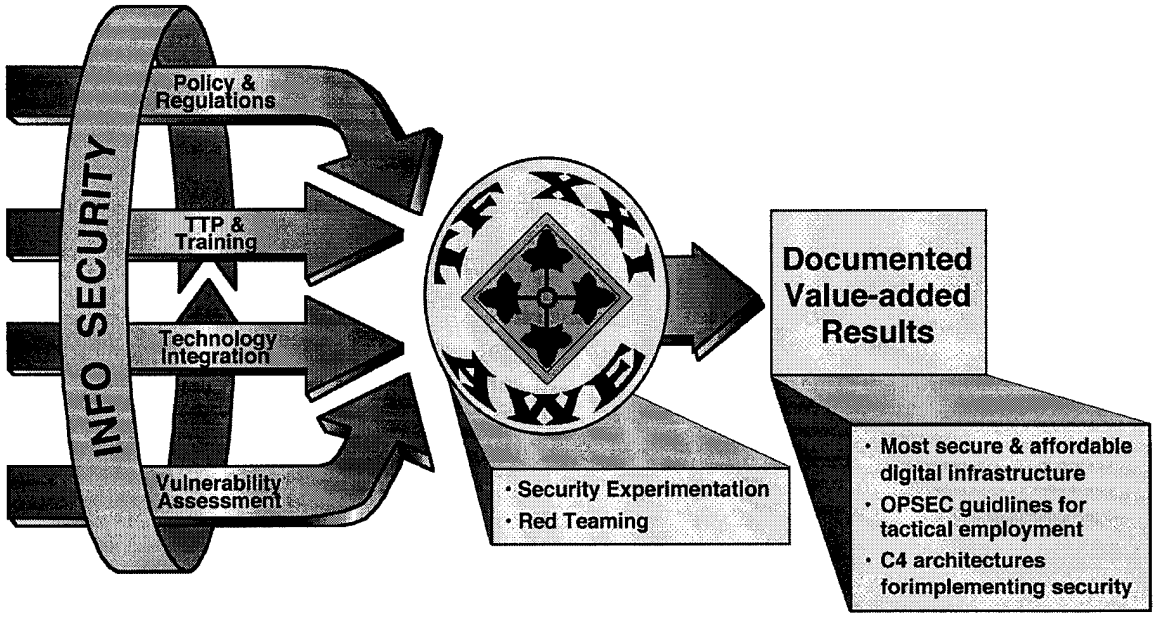


Figure 9-2 Digital System Security Approach

9.3.2 ADO Information Security Approach

To manage and/or address all ongoing actions necessary for providing information security to the digital battlespace, the ADO has divided the overall security effort into four general activities:

- Policy and regulations.
- TTP and training.
- Technology integration.
- Vulnerability assessment.

Near-term efforts are focused on successful conduct of the TF XXI AWE. Fundamental to this approach is a continuous risk management process led by the ADO to:

- Address relevant current threats being worked by the supporting DCSINT Threat WG.
- Consider trade-offs between the general activities.
- Prioritize supporting actions.
- Decide on appropriate security protection features (e.g., procedures, devices, management) that can be implemented at acceptable cost and risk.

The Army is currently addressing broad information security requirements and efforts in its Command and Control Protection (C2 Protect) Program. ADO security-related tasks are accomplished both *within the context of* and *in support of* this program. The C2 Protect Program is a fundamental portion of the new concept of *Information Operations* which is being developed to capitalize on *information age* technologies. The security lessons learned in TF XXI will provide significant input to this program and subsequently to the future security of Force XXI.

During the conduct of the TF XXI AWE, specific experimentation will be conducted in the areas of the four general activities. *Red Teaming* will be conducted in support of vulnerability assessments. Lessons learned from experimentation and applied to improved security measures will lead to a more secure digital infrastructure. The C4I architectures must incorporate and document these results to enable implementation in future systems (see Figure 9-3).

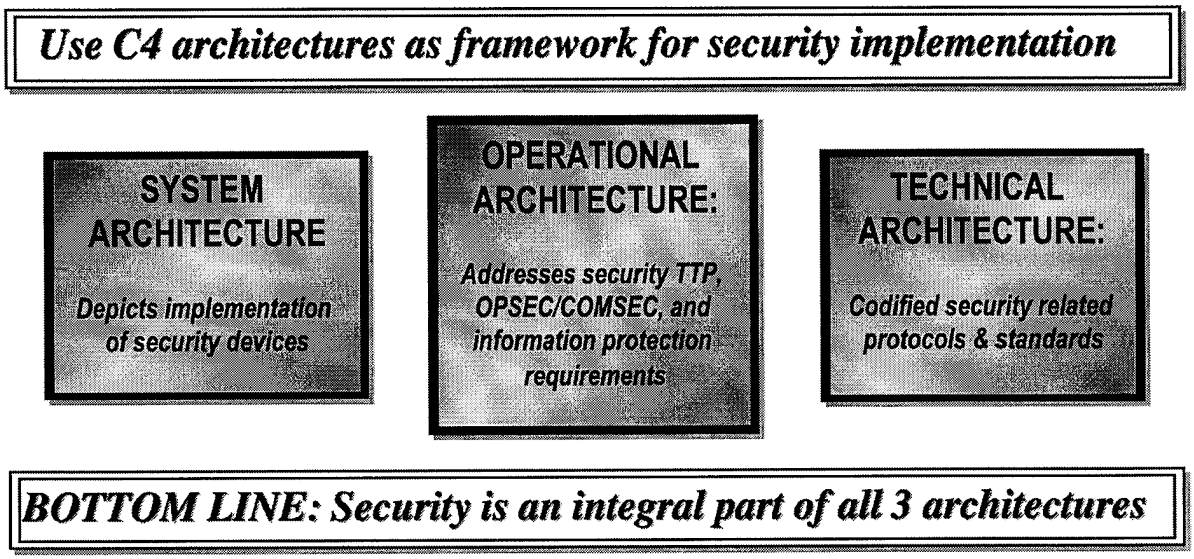


Figure 9-3 ADO Information Security Implementation

9.3.2.1 Security Risk Management

Digitization security will be *risk-based* rather than *rule-based*. The old rule-based methodology demanded that lock-tight security be maintained by stringently meeting global security rules (regulations). In the explosion of technology, such rules are no longer effective in protecting information. Costly, rule-based information systems with less capability than projected systems have been unable to provide the level of protection required because the rules have been unable to keep up with advances in technology. Risk-based systems being implemented for the digital battlespace are the result of extensive examination of realistic security requirements; tradeoffs between device-provided security and other security means; and acceptance of reasonable security risks adapted to the real-time environment of these digital systems. Through its risk management process, the ADO intends to expedite the development and implementation of information-age capabilities while knowingly accepting some inherent risks in the process.

9.3.2.2 Policy/Regulations

Policy and regulations are being reviewed to determine their applicability within the digital battlespace. Subsequent modification may be necessary to accommodate the operation of digital systems in a fast-moving tactical environment in which information is extremely time sensitive, critical to current operations, and may not meet current security requirements. If policies and regulations are not modified, capabilities will be significantly curtailed or operational commanders may have to exercise their authority to waive the restrictive rules which—if not thoroughly addressed beforehand—could cause needlessly large security risks.

The ADO intends to guide and oversee the development of modified policies and regulations in coordination with the DCSINT to accommodate the security needs of this new technology.

9.3.2.3 Tactics, Techniques, Procedures (TTP) and Training

TTP and training in the security realm are extremely important in mitigating security risks inherent in the digitized battlespace. They serve as a realistic means of offsetting the need for other security products that may be too costly to implement on a widespread basis (such as current in-line network encryptors) or that may not currently be available (such as multilevel security products).

TRADOC and the EXFOR are responsible for developing and implementing these TTP and training programs within guidance provided by the ADO. TTP developed from the Focused Dispatch and Warrior Focus exercises will be available for the TF XXI AWE.

9.3.2.4 Technology Integration

Digital technology integration has been a primary mission of the ADO since its inception. *Security technology* integration is just as important to the overall ADO mission and is being addressed as a separate, complementary entity. Many of the related ADO security actions are directed toward researching, analyzing, and ranking evolving military and commercial security technologies and then incorporating subsequent recommendations into the System and Technical Architectures as appropriate.

9.3.2.5 Vulnerability Assessment

Vulnerability assessment is important to the overall security effort. It addresses the weaknesses of current systems—to include the human element—as well as the ability of new security concepts to accomplish their intended purpose. In the context of current threats, it also is a fundamental driver for security requirements.

Guidance from the Defense Science Board (DSB) and OSD has stressed the importance of determining information system vulnerabilities and capabilities when making implementation decisions. The ADO will continue to direct a number of actions in this area (see Section 9.3.4).

9.3.3 Basic Information Security Requirements

9.3.3.1 Mandate vs Objective

Rules—in the form of security policies and regulations—still exist. In the rules-based methodology from which current information security requirements emanate, those rules are *mandates*. In a risk-based methodology, they provide information protection *objectives*. The difference is significant, providing needed flexibility for intelligent trade-offs between security and capability.

9.3.3.2 Information Protection

Information on the battlespace that is important to the employment and effectiveness of friendly forces must be protected from exploitation, corruption, and denial actions by opposing forces.

This information is given a classification level—or label—according to the criticality of that information to friendly forces and the level of damage that could be inflicted by the opposing forces if the information was available to them. Classification labels are currently applied to output (e.g., messages, reports, documents), but classification labeling is gradually evolving to labeling of the data elements themselves.

Systems which transport or process such information must provide the necessary level of protection through security devices, routines, procedures, or related means. Such systems must be certified (proven) and accredited (approved) in accordance with the provisions of AR 380-19. Similarly, a system-of-systems must provide proper protection at the individual system level as well as at the interfaces between the systems. Personnel who use this information or who have access to information through system operations must also be properly cleared for that access. When properly addressed on a total system basis, these individual requirements provide the necessary protection for the information itself. As an additional requirement, the protection of information—and systems themselves—from denial actions ensures that the information is available for its intended use.

9.3.3.3 Closed System Constraints

Unfortunately, today's information systems have not been designed to handle individual information message or data element segments on the basis of their individual classifications and then route them accordingly. A current system must handle all information segments on a *closed system basis* as if those segments were all classified at the highest level that the system is approved to handle. This precludes the ability to interface systems of different classification levels for the purpose of automatically exchanging information at a lower level of classification, even though both systems can and do process information that is actually at that level.

For example, a system that processes sensitive but unclassified information cannot automatically send—or *write–up*— unclassified information to a system that processes SECRET information. Similarly, a system that processes SECRET information cannot automatically send—or *regrade*— unclassified information to a system that processes unclassified but sensitive information. This is

due to difficulties in trusting the systems to accomplish those processes correctly without compromising the resident information not transmitted. Operators can manually accomplish write-ups and regrades, but systems cannot do so until the NSA approves certain multi-level security (MLS) products which are currently in development. This poses severe constraints in an automated information system-of-systems which relies on automatic routing and data transfer—without operator interference—to attain near real-time receipt of critical battlefield information.

9.3.3.4 Protection Requirements

The overall Army digitization security requirement is to apply current and state-of-the-art practices, designs, and security devices to the systems being deployed for Force XXI and supporting experiments in such a manner as to ensure that information protection—from both compromise and denial—is provided to an acceptable level of risk. This applies to systems being developed specifically as a part of the digitization effort (e.g., appliques, INCs, TMGs) and to existing legacy systems that will become a part of Force XXI.

9.3.4 Army Digitization Information Security Actions

To conduct the four general security activities—policy/regulations, TTP/training, technology integration, and vulnerability assessment—the ADO is working on several individual security tasks:

- System security design.
- System vulnerability assessment.
- System design analysis.
- *Red Teaming.*

All contribute to the development of secure digitization infrastructure designs and security inputs to the three digitization architectures to meet Force XXI security requirements. In the near–term, this security effort must be focused on the system design for TF XXI.

9.3.4.1 System Security Design

Information system security mechanisms have been evolving toward increased capabilities in parallel with the information systems they are designed to protect. NSA has been working to achieve multi-level security capabilities through its MISSI, which is now beginning initial production of INEs for end-to-end protection on packet networks and Fortezza cards for e-mail protection. Industry and commercial enterprises are also improving commercially available devices such as *firewalls* and *security guards,* while write-up and regrade capabilities discussed earlier are emerging in various prototype forms.

To provide proper protection of digital information on the future battlefield, PEO C3S has been tasked to develop the security overlay for the TF XXI system design. This overlay will incorporate existing security mechanisms such as COMSEC devices, security procedures, firewalls, and INEs

to accomplish necessary operational system protection and security device prototypes for experimentation. The security overlay will be key to ensuring no sensitive information is compromised, while at the same time allowing sufficient connecting interfaces for accomplishing overall situational awareness system objectives.

9.3.4.2 System Vulnerability Assessment

The second task is assessment of individual system vulnerabilities to information exploitation, corruption, and/or denial though the study of technical/operational test data and empirical operational data. This task has been assigned to the Army Research Laboratory's (ARL) Survivability/Lethality Analysis Directorate (SLAD) which is the recognized expert in this area. This is a continuing task which was initiated in 1994 and periodically provides reports of significant value to PEO C3S, the System Design Engineer. The effort involves studies of existing data as well as the conduct and evaluation of specific system testing in the areas of information, electronic, and physical vulnerabilities.

9.3.4.3 System Design Analysis

The third task is identification of specific security issues through analysis of the TF XXI system design with respect to current policy and procedures. The goal is to identify issues in time to find solutions, apply fixes, and/or provide waivers prior to the TF XXI AWE in FY97. DISC4 was given this task on 22 March 1995, and the initial review was provided to the ADO in September 1995. The issues identified in that initial review are being addressed by the ADO and the TF XXI Security IPT which is discussed later in this section.

9.3.4.4 *Red Teaming*

The fourth task is the operational *Red Teaming* of the system design. This task is designed to determine system vulnerabilities through *opposing force-like* actions (see Figure 9-4). Red Teaming of TF XXI information systems will be incorporated into all digitization exercises leading to Force XXI which appear to be potential Red Teaming opportunities. This task will incorporate the results of the tasks assigned to SLAD and DISC4, as described above, to make more global recommendations to the digitization system design.

Red Teaming will require a highly controlled process to ensure the effort is complete and addresses all operational vulnerabilities (see Figure 9-5). The C2 Protect Council of Colonels (C2PCOC) and the C2 Protect General Officer Steering Committee (C2P GOSC)—with membership from the ADO, DISC4, DCSOPS, and DCSINT—provides guidance, priorities, and resolution decisions. A number of working groups support the necessary analyses and provide recommendations. The ADO and the supporting TF XXI Red Team Working Group provide the supervision and coordination mechanism to manage the process.

Red Teams will be task organized as necessary to accommodate specific events. Operations will be conducted in conjunction with scheduled testing, training, and experimentation. There are four primary Red Team opportunities in the near-term during:

- Planned system tests.
- EXFOR train-up exercises/events.
- DIL certification of TF XXI systems.
- TF XXI NTC Rotation 97-05.

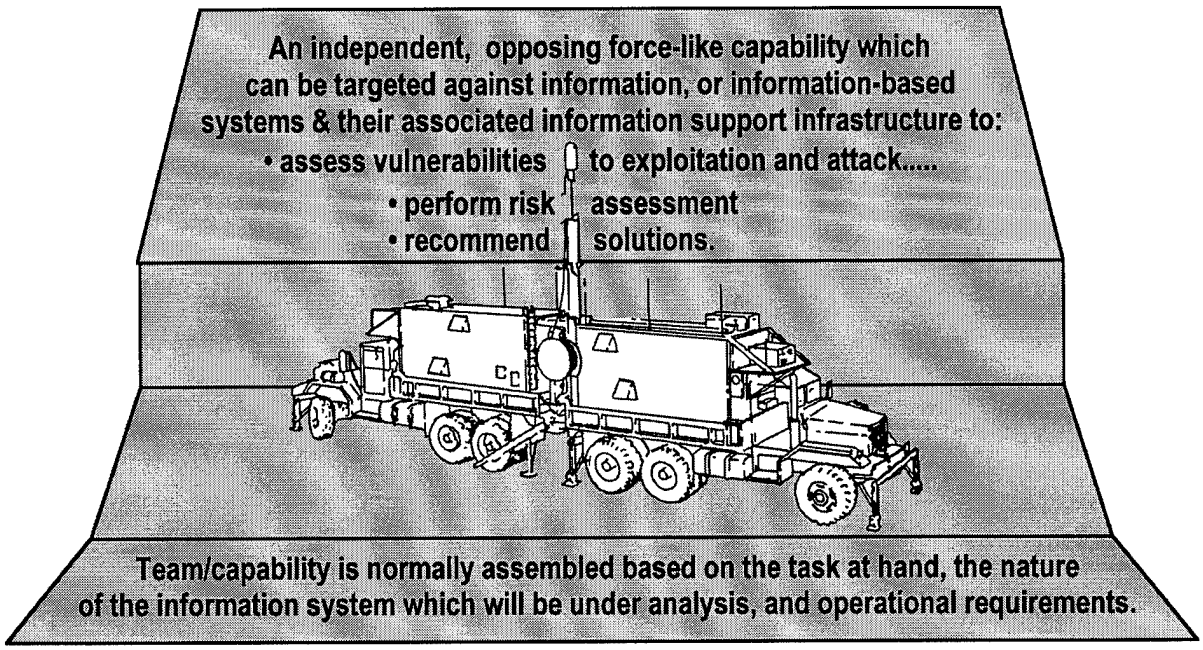


Figure 9-4 Red Team (Working) Definition

The ADO will provide day-to-day direction to organizations assigned to conduct the actual Red Teaming efforts, which for TF XXI are focused on six assigned sub–tasks:

- **Position/navigation vulnerability assessments**. The Electronic Proving Ground (EPG) will determine the ability of the network to react to loss of the GPS signal and develop initial offsetting operator TTP.

- **Non-traditional threat vulnerability assessments**. The DISA Center for Information System Security will determine the vulnerability of the TF XXI network to hackers, viruses, and other non-traditional network threats.

- **Operational Security (OPSEC) assessment**. The Land Information Warfare Activity (LIWA) will conduct a multi-discipline counter-intelligence (MDCI) OPSEC assessment to determine new/increased OPSEC vulnerabilities due to battlefield digitization/automation.

- **Security policy assessment**. DCSINT will assess the need for revised and/or additional security policy due to digitization implementation.

- **Technical component analyses**. ARL's SLAD will conduct technical experiments and analyses to determine unique vulnerabilities of the *Tactical Internet*'s individual systems.

- **SIGINT/MASINT (Measurement & Signal Intelligence) characterization assessment.** LIWA will determine patterns and signatures unique to the digitized force that may have intelligence value to hostile forces.

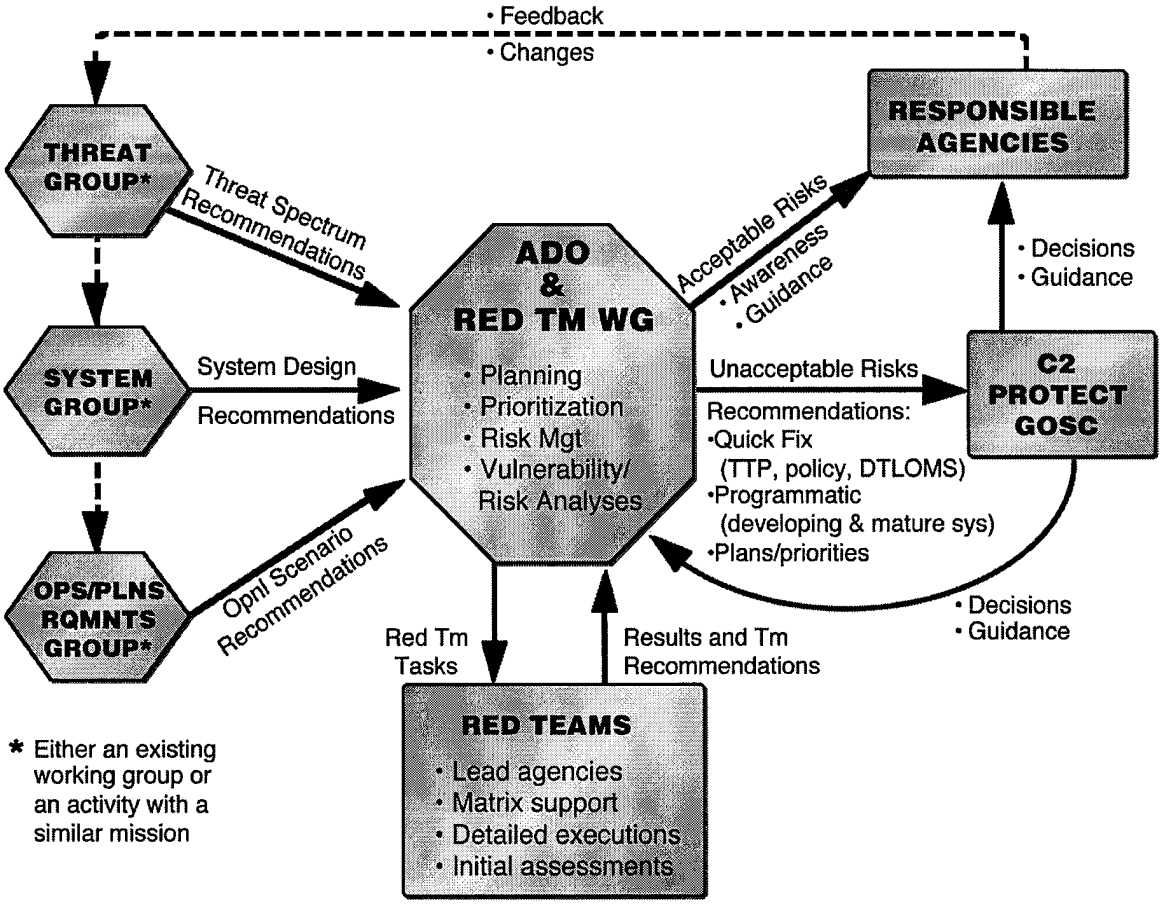


Figure 9-5 Digitization Red Team Process

9.3.4.5 Additional Security Actions

Although the previous six sub–tasks are primarily oriented on vulnerability assessments, the responsible agencies will also provide recommendations for resolving discovered weaknesses and security issues. These recommendations will be considered by the ADO; analyzed in terms of cost and benefits; and submitted to the system architects and/or engineers for action.

DISC4 is conducting a separate task to improve the incorporation of security into systems under development. This task involves the creation of security standards for inclusion in the TA, thus providing necessary guidance for system developers and improving the likelihood of interoperability between the system and its security means.

9.3.4.6 Task Force XXI Security Integrated Product Team (IPT)

In order to expedite the security process for TF XXI, a Security IPT (SIPT) has been formed by agreement of TRADOC, ADO, and DCSINT. The ADO chairs the SIPT and all agencies with security involvement provide representatives. The IPT addresses major information security issues brought to its attention, and assigns a responsible agency to take the lead on each.

9.3.5 Organization for Security Task Execution

The organizational relationships for conducting security tasks in support of TF XXI digitization are shown in Figure 9-6. Although the described tasks are predominantly accomplished by Army activities, they must accommodate the requirements of other Services, as well as provisions of guidance and regulations published by other DoD agencies.

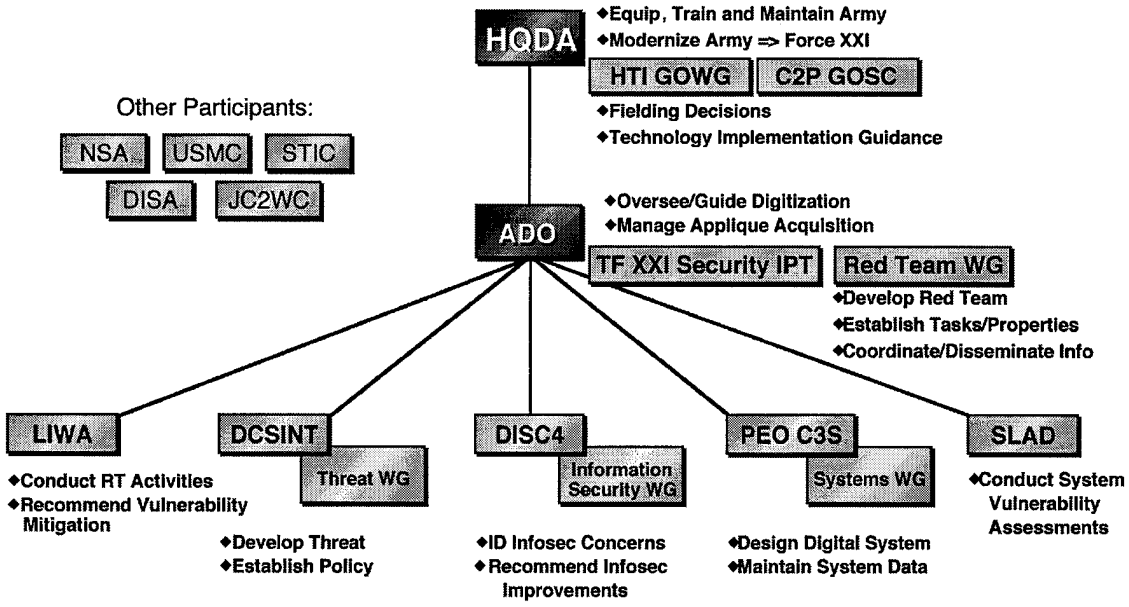


Figure 9-6 Digitization Security Task Execution

A number of other WGs and CoCs have been established to address various information security needs for both the Army and DoD. These include the C2 Protect Working Groups (C2PWGs), the beforementioned C2PCOC, and the Army Battle Command System Security Working Group (ASWG). In order to ensure optimum information security progress and synchronization of all Army information security developments, it is important that the ADO and other activities involved with digitization have representation at these groups. This will provide WGs and CoCs with the benefit of hands-on and field experience as they attempt to establish future directions for information security, while the digitization community will benefit by using the latest concepts as they are developed by these groups.

9.4 Spectrum Management

The transfer of information in the digitized battlespace is almost totally dependent on using the radio frequency (RF) spectrum as the transfer medium. Battlespace sensors and weapons systems also make increasingly extensive use of the RF spectrum. Simultaneous use by joint /multinational forces, commercial/civil systems, and the enemy poses a potentially confusing and disruptive obstacle to the essential goal of achieving and maintaining *spectrum supremacy*. Consequently, the RF spectrum becomes as critical a domain in the digitized battlespace as the other battlespace dimensions. Spectrum supremacy will be assured through a rigorous approach to achieving spectrum supportability of each and every RF-dependent system that conducts digital information transfer, from the *Tactical Internet* to AGCCS.

Spectrum supportability in the digitized battlespace must be addressed by balancing multiple factors such as bandwidth, power, spectrum availability/accessibility, spatial parameters, temporal parameters, electromagnetic wave behavior, electromagnetic environments, regulatory provisions, technical restrictions, and national and multinational variations of each. While these issues will not change appreciably as a direct result of digitization, the manner in which the digital RF systems will drive spectrum use requirements will have a dramatic impact on spectrum management technology and practices. The introduction of COTS and NDI procurements, along with new digital system acquisitions, have already served notice that the RF systems within future digital battlespace will:

- Be processor driven and controlled.
- Be adaptive in wide range of system parameters (power, modulation, and frequency).
- Use varied digital waveforms.
- Render obsolete the current spectrum management practices and procedures founded on well-defined allocation tables and discrete, channel-based frequency assignments managed by a centralized authority.

9.4.1 Spectrum Supremacy Strategy

As digital battlespace evolves, the electromagnetic environment will be faced with increasing numbers of self-managing, non-conventional systems. The challenge is to re-engineer spectrum management processes and procedures so that increased emphasis is placed on pre-acquisition system designs to assure spectrum supportability of digital systems, while less emphasis is placed on manual, post-acquisition management of system parameters during operations.

Achieving the scope and meeting the requirements of vertical and horizontal battlespace integration in will require increases in the information capacity and adaptability of RF communications systems. Each increase in system capacity or adaptive characteristics will have consequences directly relating to spectrum requirements. Re-engineering the spectrum management process to achieve spectrum supportability for the next generation of RF systems

designed to carry the digitized battlespace information flow will require the ability to predict the interactions of systems in the electromagnetic portion of the battlespace.

This process can be accelerated by aggressive adaptation of lessons learned from the Force XXI AWEs. Technical data and information derived from equipment specifications, engineering analyses, lessons learned, and feedback from exercise spectrum managers and AWE units will be used for revising spectrum management techniques, requirements, and far–term strategies.

9.4.2 Spectrum Support to the Battlefield Information Transmission (BITS) System

The BITS acquisition strategy must process its commercial system spectrum requirements through the spectrum supportability process in accordance with AR 5-12, *Army Management of the Electromagnetic Spectrum.* The spectrum supportability objective is to validate that the equipment meets technical parameters and specifications which permits the equipment to operate within the designated spectrum. Approval provides accessibility to frequencies for operations in the U.S. and worldwide, but the certification process is complicated because friendly nation approval must be obtained prior to actual operations and their frequency spectrum allocations are not necessarily consistent with U.S. allocation tables. Consequently, early planning and coordination facilitates spectrum supportability in the Pacific and European theaters.

RF requirements for systems supporting the *Tactical Internet* will rapidly evolve beyond the ability of current practices and procedures to deal effectively with spectrum supportability issues. The NTDR will be the first in a series of multiple evolutionary steps that will change the behavior of RF systems in the battlespace. The acquisition strategy must include consideration of the role of spectrum certification in the face of new, potentially unconventional, and potentially *non–compliant* technologies.

The role of spectrum certification in the acquisition strategy must also be reexamined to consider the introduction of processor-driven, adaptive RF technologies. The RF systems that will be introduced as a necessary adjunct to the battlespace digitization effort will also introduce waveforms and parameter variations that are not considered in the certification process for conventional systems.

Adherence to technical standards and allocations will be challenged in many designs. These challenges must be met objectively, with a clear and consistent view of how future digital RF transmission systems can best serve the objectives of the digitized battlespace without causing disruption and chaos in the electromagnetic environment.

9.4.3 Spectrum Supportability, Multinational Strategy

Spectrum supportability from an allied nation with different or more stringent standards than the U.S. can become a significant obstacle to equipment fielding and operational use. These difficulties were experienced in the 1980s when the U.S. introduced JTIDS, REGENCY NET and SINCGARS into the multinational arena. Spectrum compatibility has historically proven to be a difficult challenge in Germany, Japan, and South Korea.

These challenges will grow as the Army digitization plan introduces equipment and systems that do not necessarily adhere to clearly defined—but obsolete—allocation tables. A dynamic mix of new conventional and adaptive digital systems will be introduced over the next decade into a multinational arena in which understanding and acceptance of advanced, processor-driven digital RF technologies will vary from country to country. Electromagnetic compatibility and interoperability at the RF–level will thus become critical issues within the multinational strategy.

9.5 Training

The full integration of digitization in the battlespace will only be possible with timely, effective training of soldiers, leaders, and units. Training initiatives associated with *Joint Venture*—Warfighter, Warrior, Warnet—must address operation, employment, and maintenance of the digital equipment. PEOs and CECOM, in coordination with TRADOC, are responsible for developing EXFOR training programs. Training development will follow the Army systems approach to training and must be compatible with current Army automated training development and information systems.

The ADO will synchronize combat, materiel, and training development of digitization hardware and software systems. Existing live, virtual, and constructive (L/V/C) training systems will be upgraded to integrate digitized systems, and future training systems must be developed with digitization as an integral design aspect. Structured training programs must be developed for L/V/C automated training systems to ensure progressive, sequential training of all relevant tasks, conditions, and standards. Training systems supporting digitized hardware and software must be designed, developed, tested, and ready to field with the equipment at FUE.

TT/OTs, AWEs, and supporting evaluations will include tests of embedded and supporting training and training systems to ensure timely fielding of training packages consistent with operational and training requirements. Training and training development will become an integral aspect of life–cycle cost estimating to ensure adequate, timely resourcing of required training aids, devices, simulators, and simulations (TADSS) and embedded training systems. Training will also become an integral aspect of configuration management to ensure compatibility and interoperability of operational and training systems.

Digitization adds a new dimension to battlespace command and control that must be analyzed, assessed, and evaluated to determine its most effective use. Functional information and lessons learned must be inserted into TTP. Digitization doctrine and technical information must be integrated into existing and future doctrinal publications, soldier training publications, *Army Training and Evaluation Program (ARTEP) Mission Training Plans*, automated training and training development systems, institutional training, and unit training strategies and plans.

Total Army digitization training will begin with training in support of TT/OT or NET and progress to become integral to Force XXI training programs at the individual, institution, and unit levels using a mix of L/V/C training techniques. Institutional training and training support requirements must be identified and resourced early in the digitized system's life–cycle to ensure availability of training support prior to FUE.

- Techniques will include use of embedded training, multimedia training (e.g., distant learning, computer-based instruction, and training video tapes), TADSS, hands-on training, and collective training of tasks from the team/crew/section level through EAC.

- L/V/C simulations will be conducted using a combination of embedded training and existing/future simulations and simulators linked in STOW unit training exercises.

- Embedded and stand alone training systems will be designed to provide both immediate and deliberate evaluation as part of the Standard Army After Action Review System (STAARS).

- Training will be conducted on the system, in learning centers, in classrooms, in simulation centers, in motor pools, in local and major training areas, and at Combat Training Centers (CTCs).

- Training developments will follow the Systems Approach to Training (SAT) and be compatible with the Automated Systems Approach to Training (ASAT) and the Standard Army Training Systems (SATS).

10. JOINT AND MULTINATIONAL DIGITIZATION

10.1 Joint

The focus of the Army to attain joint interoperability in the digitized battlespace has three components.

- First, the Army and the other Services are working to achieve technical interoperability by migrating their current C4I systems to the Joint Staff's *C4I for the Warrior* concept. In accordance with the migration, the ADO will coordinate Army efforts to ensure that the ATA for information systems is in compliance with the DII COE.

- Second, the ADO will closely coordinate digitization efforts, to include the review and approval of information standards and data transport profiles, with the other Services, the Joint Staff, and OSD through MOA and proactive participation in joint working group panels that comprise the MCEB. To ensure senior level involvement from the other Services, the HTI GOWG will invite appropriate flag rank personnel from the other Services when joint interoperability issues are scheduled for discussion. This is in addition to the other-Service flag rank personnel that make up the membership of the newly created Joint Battlefield Digitization GOWG.

- Third, other Services will be invited to participate in planned AWEs, BLWEs, and other experiments. These events will be used to identify, address, evaluate, and resolve interoperability effectiveness issues.

10.1.1 Memoranda of Agreement (MOA)

Bilateral MOAs have been signed between the Army and the other Services to focus their interoperability efforts. The MOAs express each Service's senior leadership's full support for achieving interoperability in the digitized battlespace. The MOAs define Service digitization efforts and describe the management structures used to monitor, coordinate, and guide the efforts of each Service to achieve joint interoperability.

The goal of each MOA is to establish mutual, cooperative development that will achieve integration between the digitized forces of each Service on future maritime, air/space, and land battlefields/battlespace at all echelons of command. The objective of the MOAs is to achieve interoperability among the Services across all three architectures—Operational, System, and Technical—through compliance with the DII COE. Management structures defined in each MOA enable operational and system interoperability issues to be identified and resolved. The efforts of each Service are interrelated, allowing Service-specific mission applications while ensuring interoperability among all Services.

As part of the MOAs, the other Services are authorized and encouraged to conduct direct liaison with TRADOC, AMC, OPTEC, and the AAE structure for exchange of technical, user, and

operational requirements to further define and scope unique interoperability tasks and requirements. Both the ADO and the other Services will effect liaison with each other to ensure frequent opportunities for dual–Service interaction and expeditious resolution of problems, issues, and conflicts.

10.1.2 The Military Communications and Electronics Board (MCEB)

The MCEB coordinates military communications and electronics matters among DoD components and is the key organization to obtain resolution of interoperability issues. The ADO will work within the MCEB structure of functional panels and working groups to obtain Joint/OSD approval of Army digitization interoperability efforts. Since the MCEB review and approval process is extensive and lengthy, the role of the ADO will be to obtain consensus among the Services through MOAs, WGs, and fora of flag rank level personnel prior to submission of the issue to the MCEB process. This expeditious *front loading* of the review/approval process is necessary to ensure that the process of achieving joint interoperability is on a parallel timeline with the aggressive Force XXI milestone schedule.

10.1.3 Management Structure

A three-tier management structure is used to identify issues and problems requiring resolution. At the top tier, the Joint Battlefield Digitization (JBD) GOWG is responsible for providing direction to the overall interoperability efforts of the Services. It meets as required to resolve conflicts; establish priorities in resources and direction of digitization development; and assist in the coordination and execution of battlefield/battlespace digitization initiatives.

Membership in the JBD GOWG is defined in the MOAs as follows:

- Army:
  - Director, Army Digitization Office.
  - Deputy Chief of Staff (Combat Development), TRADOC.
  - Deputy Chief of Staff for Operations and Plans (Force Development), HQDA.
  - Deputy Director, Information Systems for C4.
- Navy:
  - Director, Space and Naval Warfare Systems Command (SPAWAR/30).
- Air Force:
  - Director of Requirements (AF/XOR), HQ USAF.
  - Director of Mission Systems (AF/SCM), HQ USAF.
  - Director of Fighter, Command and Control, and Weapon Programs (SAF/AQP), Office of the Secretary of the Air Force.
- Marine Corps:

- Commander, Marine Corps System Command (MARCORSYSCOM).
- Deputy Commander, Marine Corps Combat Development Command (MCCDC).

The middle tier consists of a JBD Council of Colonels/Captains (CoC/C) with members from each of the Services. This CoC/C is responsible to identify issues and problems; make recommendations to the JBD GOWG; and ensure that the GOWG's direction is implemented. The Council meets at least quarterly. Minimum membership consists of a materiel developer, a combat developer, and a budget/funding member from each Service. Additional Colonels/GM15s from OSD, the Joint Staff, and other programs attend as non-voting members and observers.

The bottom tier consists of a series of WGs comprised of action officers and subject matter experts from each Service. The groups are responsible for monitoring of digitization efforts and gathering of information in response to GOWG and CoC/C issues. These groups are:

- Training
- Architectures
- Evaluation and Assessment
- Service Participation in TF XXI
- Communications/Data Links
- ATCDs

A series of interoperability issues have been identified and assigned to the appropriate working group for resolution. Additional ad hoc working groups are formed as required by the CoC/C.

10.1.4 Joint Initiatives and Experiments

The ADO will use planned digitization experiments to evaluate and assess joint digitization efforts. The first target of opportunity is the TF XXI AWE in 1997.

All other Services are invited to participate in TF XXI. Each Service will develop its experimental objectives that will be reviewed and incorporated in the Army's experiment concept (See Section 8.1.2.8). Based on the extent of participation, each Service will receive a sufficient number of software and hardware appliques through the Army's FBCB2 contract to ascertain interoperability connectivity and compatibility. Based on the results of this AWE, a baseline for joint interoperability will be established and used as a comparison for joint interoperability during follow-on AWEs.

There are many opportunities for leveraging digitization programs of other Services. The Army intends to make full use of JWIDs to assess interoperability in the joint digitized battlespace, and the ADO will coordinate with the other Services to identify applicable digitization initiatives and concepts. The Air Force has identified approximately 75 concepts that apply to the digitized battlespace. They include communications, navigation, identification, information management, and Local Area Network (LAN)/Wide Area Network (WAN) functions. The Navy and Marine Corps are also being surveyed for potential digital battlespace concepts that can be evaluated by the Army for possible inclusion in AWEs and/or ATDs. Resulting data will be made available to the Services through management and coordination structures previously described.

The Army's DIL provides the preliminary examination of prototype hardware and software to verify ability to perform critical functions and meet interoperability requirements. The DIL is accessible to all the other Services, with the Marine Corps slated to be the first to link with it. The DIL will also be connected to selected multinational partners. Use of the DIL will be based on an incremental concept of *build a little, test a little.*

10.2 Multinational

10.2.1 Background

Faced with the challenge of maintaining and modernizing military forces to meet a variety of unpredictable worldwide threats, the U.S. will rely heavily on multinational cooperative actions to meet future mission requirements. DoD Directive 4630.5 states that forces for joint and multinational operations must be supported through compatible, interoperable, and integrated C4I systems that can support operations worldwide throughout the entire spectrum of conflict. As Army plans for digitizing the battlefield move forward, this requirement becomes more pressing.

TRADOC Pamphlet 525-5 (*Force XXI Operations*) states as a goal that these operations be conducted under conditions where U.S. forces— supported by coalition partners, enjoy a qualitative technical, training, leadership, and, most important, information advantage. Digitizing the battlefield—one of the objectives of the *Army Enterprise Strategy*—will lead toward the realization of this goal by providing an integrated digital information network to support warfighting systems and ensure command and control decision-cycle superiority.

Digitization efforts must also be aligned with the *Army Enterprise Implementation Plan*, which is based on the current and evolving doctrine emanating from Field Manual 100-5 (*Operations*).

10.2.2 Purpose

The *International Digitization Strategy* (*IDS*) is designed to focus the international activities of the Army in support of the goals and objectives outlined in the *ADMP*. The *IDS* comprises the overall strategy for international cooperation in the application of doctrine and technology to facilitate acquisition, exchange, and employment of digital information throughout the combined battlespace. The priorities and processes outlined in the *IDS* will enhance the ability of the U.S. and its coalition partners to field inherently interoperable systems.

10.2.3 Concept

The concept for achieving multinational force compatibility is illustrated in Figure 10-1. It is based on the underlying concepts of adopting commercial standards to achieve open systems; using existing C4I fora to promote the integration of the Army's digitization initiatives; leveraging foreign advances in technology; and pursuing the application of emerging technologies to support coalition warfare and multinational operations.

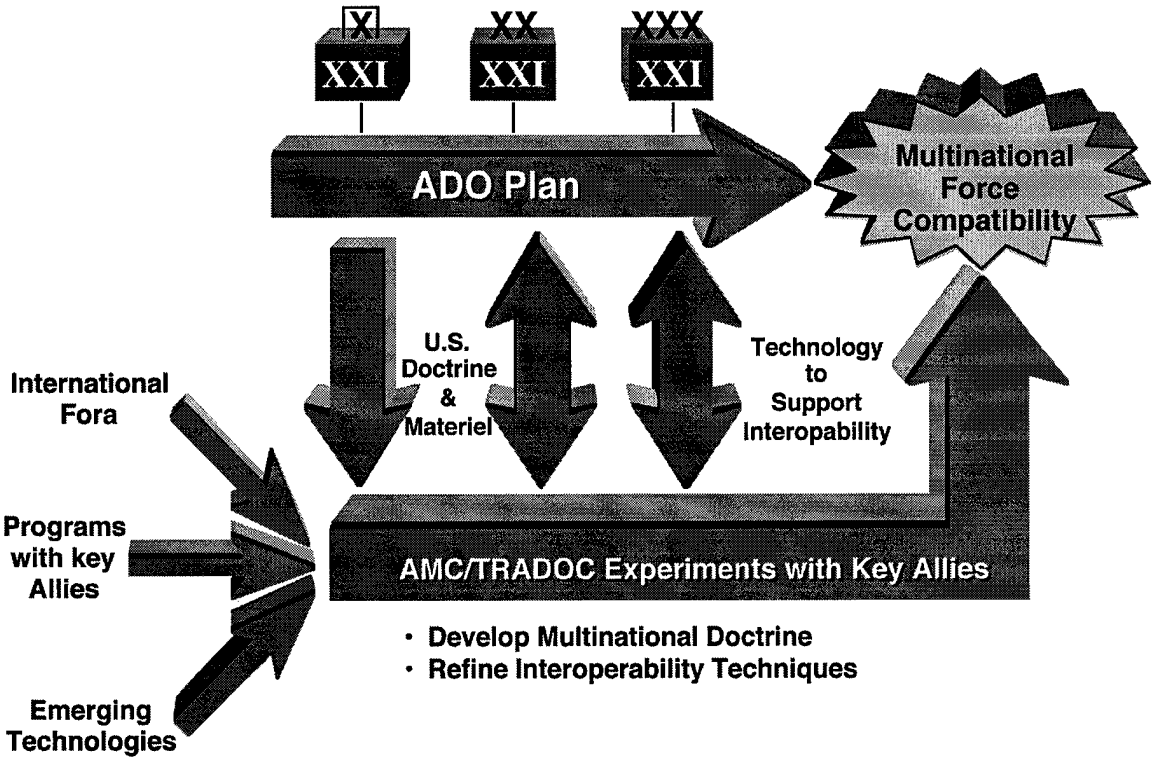


Figure 10-1 International Digitization Concept

10.2.4 Process

The *IDS* defines a systematic process to extend U.S. digitization efforts to the international arena. The process is based on establishing an understanding of U.S. digitization efforts, achieving interoperability with potential coalition partners, and pursuing long–term cooperative opportunities. The process includes a number of elements designed to:

- Define the strategy to achieve interoperability of C4I systems between key allies, to include broad agreements on policy and procedures concerning information exchange, architecture definition, and architecture development processes.

- Identify the key forum/fora in which to coordinate national digitization positions.

- Define and implement technical and system architectures applicable to all participating nations which will enable seamless information flow during coalition warfare.

- Develop cooperative multinational programs to share technology (e.g., components, systems, and standards) for the automated exchange of information.

- Establish priorities for existing international fora to further the aims identified by the Quadrilateral Army Communications and Information Systems Interoperability Group (QACISIG), which is responsible for coordinating the position of all participating nations on the passage and exchange of information between Army systems.

- Evaluate multinational C4I systems and ATD products in operational/lab environments.

10.2.5 Strategy

The specific strategy is to:

- Develop a C4I operational architecture that will satisfy operational requirements for interoperability with multinational forces.
- Focus the efforts of existing multinational fora involved with the interoperability of C4I systems on goals established by the QACISIG.
- Identify other key international fora whose efforts will contribute to meeting the goals established by the QACISIG.
- Ensure that prototype systems developed by current/planned international cooperative programs meet interoperability goals.
- Pursue the consolidation of related efforts through an annex to the *Senior National Representative (Army) Memorandum of Understanding* between the U.S., U.K., Germany, and France to facilitate the pursuit of multinational cooperative digitization projects under the coordination of the QACISIG.
- Present the ATA to international standardization groups and C4I fora through the designated U.S. representatives and—using established processes—acquaint the international community with its concept, approach, and underlying standards.
- Invite allies to observe U.S. Army ATDs, BLWEs, and AWEs.
- Use the CECOM DIL and the JITC to simulate and confirm interoperability.

10.2.6 Key International Fora

Army participation in key international fora is essential for coordination and cooperation with coalition partners. These fora provide a mechanism for harmonizing the operational, system, and technical architectures of the member armies. Participation in international fora also facilitates the leveraging of advanced and emerging technologies identified as candidates for meeting future Army requirements.

The strategy concerning international fora is to first identify key groups with the greatest potential for contributing to the digitization effort and then to focus those groups on addressing relevant digitization efforts. Figure 10-2 presents a list of these key international fora. The ADO will work with the designated lead activity for each forum to ensure that the goals and objectives of the *ADMP* and *IDS* are represented and consistently presented. The QACISIG—which includes representatives from the policy directorates of the key nations—is an appropriate forum for establishing overall goals for the international digitization process.

NATION	FORUM	DIGITIZATION PRODUCT	LEAD	COMMENT
US/GE /FR/UK	QACISIG	Interoperability Strategy (six-step process) for corps and below . Appropriate forum for establishing goals of digitization process	DISC4	AMC/TRADOC support
NATO	ATCA (Land)	Tactical communications interconnectivity	DISC4	TRADOC/SIGCEN/ USAREUR support
	TSGCE, SG/9	Variable Message Format-Tactical	DISA/JIEO	CECOM participation
	TSGCE, SG/11	Internet Standards-Tactical	DISA/JIEO	CECOM participation
	NAAG, PG/25	Battalion and below C2/NATO Digitization	CECOM	TRADOC/TACOM participation
	ATCCIS (SHAPE-sponsored)	Minimum standards for NATO Level 5 system interconnectivity: corps thru brigade	DISC4	Proof of concept demo 1QFY96 High-level data exchange demo late 96
	ADSIA	Messages & multinational message standards	TRADOC	
	ATP 4 5CWG	Automated NBC warning and reporting	USANCA	TRADOC support
	Combat ID WG	Demonstration 1997	PEO IEW	
US/UK/ Canada/ Australia	ABCA Quadripartite WG Comm & Info Sys	Extends standards approach for interoperability to Canada and Australia	CECOM	DISC4 participation
	TTCP/SG X	Computing Technology/Architecture	ARL	
GE/FR /UK	Staff talks	Combined doctrine (including digitization)	TRADOC	DCSOPS/AMC/ DISC4 support
GE	AAWG	Harmonization of development programs with digitization objectives	AMC	TRADOC support
FR	CEWG/TWG	Identification of cooperative programs supporting digitization	CECOM/ ARL	
UK	Home on Home	ID of cooperative technology programs	ARL	
Korea	CEWG	ID of cooperative pgms sptng digitization	CECOM	

Figure 10-2 Key International Fora

10.2.7 Major International Digitization Programs

International digitization programs promote multinational force compatibility consistent with the objectives of the strategy. Key digitization initiatives and technology opportunities have been identified and will receive the priority needed to ensure that applicable international agreements are established and implemented.

Data/Information Exchange Annexes (D/IEAs) to appropriate MOAs facilitate the exchange of information related to digitization between nations. This information is essential for identifying potential collaborative efforts and technology leveraging opportunities. D/IEAs are conducted on a *quid pro quo* basis and have clearly defined objectives.

The international digitization strategy includes a number of cooperative programs currently in place or being planned. These include:

- The Battlefield Interoperability Program (BIP) with Germany and France (formerly the International Command and Control Systems Interoperability Project (IC2SIP)).

- The Supreme Headquarters Allied Powers Europe (SHAPE)-sponsored Army Tactical Command and Control Information System (ATCCIS) project
- The Combat Identification program with Germany, France, and the United Kingdom.
- The Interoperability for Land Tactical Communications project with Canada.
- The Theater Automated Command and Control System (TACCIMS) for extending digitization in the confined battlespace of the Korean Peninsula between U.S. Forces Korea and the Republic of Korea Army.

International programs allow the U.S. to leverage the research and development investments of multinational partners. Worldwide technology trends and specific C4I technology leveraging opportunities are identified and referenced in the *IDS*. ARL's Federated Laboratory will provide dynamic avenues (e.g., teaming) for initiation and execution of international technology programs focusing on digitization.

10.2.8 Demonstrations and Experiments

A key component of the international digitization strategy is the use of demonstrations and experiments to evaluate developed capabilities in an operational environment, determine requirements for interoperability, and make allied partners aware of U.S. digitization efforts.

Multinational partners will be invited to observe U.S. Army ATDs, BLWEs, and AWEs. The TRADOC Battle Lab Integration Technology and Concepts Directorate will coordinate the scope, nature, and duration of foreign observation. Further coalition participation will be pursued on a selective basis so as not to adversely impact any U.S. program. Future multinational exercises will be designed to confirm concepts, doctrine, and technical solutions.

10.2.9 Organizational Responsibilities

The ADO has overall responsibility for implementing and executing the international digitization strategy through the Principal Deputy for Technology at AMC, its Executive Agent for International Digitization, with cooperation and support from all participating organizations.

10.2.10 Summary

The U.S. Army international digitization strategy is to extend current digitization efforts to allies and potential coalition partners through information exchange; cooperative programs; commitment to common operational, system, and technical architectures; and technology leveraging. International programs/initiatives involved in digitization will be assessed in accordance with TRADOC Pamphlet 525-5, the *Army Enterprise Implementation Plan*, and the *ADMP* to ensure that all aspects of DTLOMS and technology issues are addressed. The strategy will evolve to reflect changes in the global environment; science and technology; and political and economic forces.

Army Digitization Master Plan

EXECUTIVE SUMMARY

"Digitization is the essential enabler that will facilitate the Army of the 21st Century's ability to win the information war and provide deciders, shooters, and supporters the information each needs to make the vital decisions necessary to overwhelm and overcome their adversary and win the overall campaign."

Major General Joe Rigby

Digitization is about interoperability. It horizontally and vertically integrates the Army's diversified battlefield operating systems into an interlocking information exchange network, while also providing a heightened level of essential joint and combined interoperability within a multi-dimensional battlespace. The rapid sharing of enemy and friendly information among all digitized forces within that battlespace will provide near-real time situation awareness, enhance synchronization of combat power, and enable economy of force by making units more lethal and survivable. Victory in the 21st Century battlespace will be characterized by the effective leveraging of information technology to rapidly mass the effects of dispersed firepower, rather than relying exclusively on the physical massing of weapons and forces that was the primary method employed in the past. Digitization is a means to that end and the *Army Digitization Master Plan* is the Army's roadmap to getting there.

ARMY DIGITIZATION MASTER PLAN

The *Army Digitization Master Plan* is a living document that will be updated on an annual basis. As digitization efforts mature, the *Master Plan* will be further refined and adjusted, based on results from the extensive modeling, simulation, and experimentation built into the program.

DIGITIZATION PROGRESS

The Army has made significant progress toward the digitization effort since the first *Master Plan* was published. This progress is characterized by the following accomplishments:

- **Horizontal Integration of Battle Command Mission Need Statement (MNS).** Obtained approval, joint certification, and validation by the Joint Requirements Oversight Council (JROC) of the *Horizontal Integration of Battle Command MNS*, which was needed to support the expenditure of Research, Development, Test, and Evaluation (RDTE) digitization funds.

- **Architectures.** Spearheaded efforts to establish a comprehensive architecture for Force XXI, resulting in an approved Technical Architecture for all Army systems that produce, use, or exchange information electronically. On 1 December 1995, ASD (C3I) selected the Army Technical Architecture (ATA) as the Joint Technical Architecture baseline. Army acquisition documentation packages have been reviewed and modified to ensure compliance with the ATA, thus beginning the process of oversight and standardization across major systems. The initial draft of the Task Force XXI System Architecture has been completed and is being staffed, while the Training and Doctrine Command (TRADOC) has begun developing the process and data models for brigade-and-below operational architectures.

- **Applique Systems.** Developed the digitized applique distribution and force modernization fielding plans for the Task Force XXI Advanced Warfighting Experiment (AWE), which were subsequently approved. Additionally, the Digital Integrated Laboratory (DIL) at Fort Monmouth has begun certifying equipment and systems designated for use during the planned series of Force XXI AWEs.

- **Acquisition Streamlining.** Briefed a prototype acquisition streamlining model which was approved as the Army standard; was supported by both Congress and the Office of the Secretary of Defense; and was instrumental in completing a contract award for the applique systems in only six months. This acquisition streamlining model has become the basis for fielding follow-on Force XXI digital systems, beginning with the solicitation package for the Near Term Digital Radio.

- **Common Operating Environment (COE).** Increased the level of joint coordination and cooperation via Memoranda of Agreement with the other Services. To this end, a two-star Joint Battlefield Digitization General Officer Working Group and a Council of Colonels/Captains have been organized and hold regularly scheduled meetings. This has resulted in a better mutual understanding of the COE and the issues involved in a smooth migration to it. The COE is the set of integrated services supporting mission application software requirements across the Military Services. It provides the corresponding software development environment, architecture principles, and methodology to assist in the development of mission application software.

- **Multinational Arena.** Made significant overtures in multinational interoperability by extending the U.S. digitization effort to selected allied and potential coalition countries. The *International Digitization Strategy* seeks to develop an interoperable operational architecture for command, control, communications, and intelligence (C4I); focuses the efforts of existing multinational fora to support the goals and objectives of Army digitization; leverages existing international cooperative programs; and invites allies to observe AWEs and demonstrations. These efforts have led to discussions with many nations and the initiation of an interoperability program with Germany and France.

- **Publicity and Education.** Conducted a broad-based information and education campaign about Army digitization and its future role on the battlefield. There is now a widespread

understanding of digitization and a proliferation of new ideas and technologies to support Army XXI, the Army of the 21st Century. The Army Digitization Office (ADO) assisted in this effort by:

- Publishing the first *Army Digitization Master Plan* in January 1995.
- Establishing an interactive, HTML-based Army Digitization Home Page on the Internet (http://www.ado.army.mil).
- Developing, publishing, and regularly updating a Digitization Master Schedule which provides visibility and synchronization of major contributing programs.

EXPANDED SCOPE

In this second release of the *Army Digitization Master Plan*, particular attention is paid to providing the current status of digitization efforts. In addition, the following informational areas have been added or expanded:

- An overview of the Department of Defense (DoD) and Service interoperability programs which will eventually define the migration of Defense and Service-specific systems to the COE.
- Discussion of the Technical, System, and Operational Architectures, and the process of developing an Army architecture that is in compliance with DoD guidelines.
- Specific descriptions of Army battle command systems, along with plans to migrate them to the COE.
- A crosswalk of AWEs, specifically highlighting digitization expectations and results of completed experiments.
- An in-depth look at interoperability at the joint and multinational levels.
- An overview of related digitization functions, which include:
  - Security, with special emphasis on Red Teaming activities.
  - Risk management.
  - Spectrum management.
  - Digitization training.

C4I INTEROPERABILITY CONCEPTS

Army digitization efforts are based on the Joint Staff *C4I for the Warrior* concept, which envisions a widely distributed, user-driven infrastructure. The warrior plugs into it to obtain information from secure and seamlessly integrated computer and communications systems. The framework to meet and conquer the challenges of this concept is encompassed by the *Army Enterprise Strategy*, which focuses on the information needs of the Army as a whole. It addresses the Army's requirements to organize, train, and equip the force; the interoperability requirements as a component of a joint or multinational force; and the functional requirements for sustaining the force from both tactical and business perspectives. These documents—along with the Navy's *Copernicus*, the Air Force's *Horizon*, and the Marine Corps' *Sea Dragon* strategies—contain the intellectual basis for current and future digitization efforts.

DIGITIZATION DEFINED

Digitizing the battlefield is the application of information technologies to acquire, exchange, and employ timely digital information throughout the battlespace, tailored to meet the needs of each decider (commander), shooter, and supporter...allowing each to maintain a clear, accurate vision of the surrounding battlespace necessary to support both planning and execution.

Figure 1. Digitization Effects

The digitization picture is based on common data collected through networks of sensors, command posts, processors, and weapons platforms. This allows participants to aggregate relevant information and maintain an awareness of what is happening around and among them. Specifically, digitization provides:

- A common picture of the battlespace in near-real time (*situational awareness*).
- Shared data among and between battlefield operating systems.
- The ability to more effectively and decisively concentrate combat power.
- High-speed data exchange.
- Correlation, fusion and display of intelligence information to commanders at all levels.
- Rapid exchange of targeting data from sensor to shooter.

REQUIREMENTS

The key requirements documents guiding the digitization effort are:

- *Horizontal Integration of Battle Command (HIBC) MNS*, which establishes the baseline operational requirements for digitization of the battlespace and future command systems. The MNS was validated by the JROC on 10 January 1995.
- *Army Battle Command System: Common Operating Environment/Common Applications Operational Requirements Document (ABCS:COE/CA ORD)*, which will further refine the operating capability needs defined in the *HIBC MNS*. This document, being developed by TRADOC, calls for the migration of current Army command and control component systems into one integrated system.

Force XXI Battle Command, Brigade-and-Below (FBCB2) ORD, which defines the needed command and control capabilities down to the lowest echelons. The ORD will be refined and updated as a result of knowledge gained from the Task Force XXI AWE.

ARMY DIGITIZATION OFFICE (ADO) MISSION

The mission of the ADO is to oversee and coordinate the integration of Army battlespace digitization activities. The Director of the ADO is the Army Vice Chief of Staff's means for providing Departmental-level guidance pertaining to digitization across the major commands, while also serving as the Army Acquisition Executive's (AAE's) instrument for providing guidance, assistance, and direction in acquisition matters related to digitization.

ADO RELATIONSHIPS

The ADO functions as principal advisor to the Vice Chief of Staff and the Army Acquisition Executive on digitization–related matters. In those parallel roles, the ADO coordinates directly with the primary commands and agencies of the acquisition and user communities, to include:

- TRADOC for warfighting concepts, requirements, battle labs, AWEs, demonstrations, and functional/operational architectures.
- Army Materiel Command (AMC)/Communications and Electronics Command (CECOM) for system engineering and materiel solutions.
- Operational Test and Evaluation Command (OPTEC)/Army Materiel Systems Analysis Activity (AMSAA) for experimentation and validation support.
- Forces Command (FORSCOM) for units participating in digitization experiments.
- Program Executive Officers/Program Managers (PEOs/PMs) for managing the acquisition of digitization and supporting communications hardware, software, and systems engineering support from AMC.
- Army Major Commands (MACOMs), other Services, and multinational partners for coordinating digitization efforts and receiving feedback on the utility of those efforts.

The AAE is the Army's Technical Architect for all information systems. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) supports the Technical Architect by developing and maintaining the technical architecture for both battlespace systems and installations. The Director of the CECOM Research, Development and Engineering Center (RDEC) is the Systems Engineer, providing technical support to the DISC4. The ADO ensures that all digital efforts are compliant with the technical architecture.

ARCHITECTURE

The Army's approach to improving its capabilities across the spectrum of potential scenarios is to develop architectures from the views of operational requirements, system capabilities, and technical standards. These three architectural views are termed the Operational, System, and Technical Architectures, as depicted in Figure 2.

- **Operational Architecture (OA)** is a description which defines the force elements and the requirement to exchange information between these force elements. It defines the types of information, the frequency of information exchange, and which warfighting tasks are supported by these exchanges. It also specifies what the information systems are operationally required to do and where these operations are to be performed. TRADOC is the Operational Architect for Force XXI.

- **System Architecture (SA)** is a description of the systems solution used to satisfy the warfighter's operational architecture requirement. It defines the physical connection, location, and identification of nodes, radios, terminals, *et al* associated with information exchange. It also specifies the system performance parameters. The system architecture is constructed to satisfy operational architecture requirements according to the standards defined in the technical architecture. The Program Executive Officer for Command, Control, and Communications Systems (PEO C3S) is the System Architect for Force XXI.

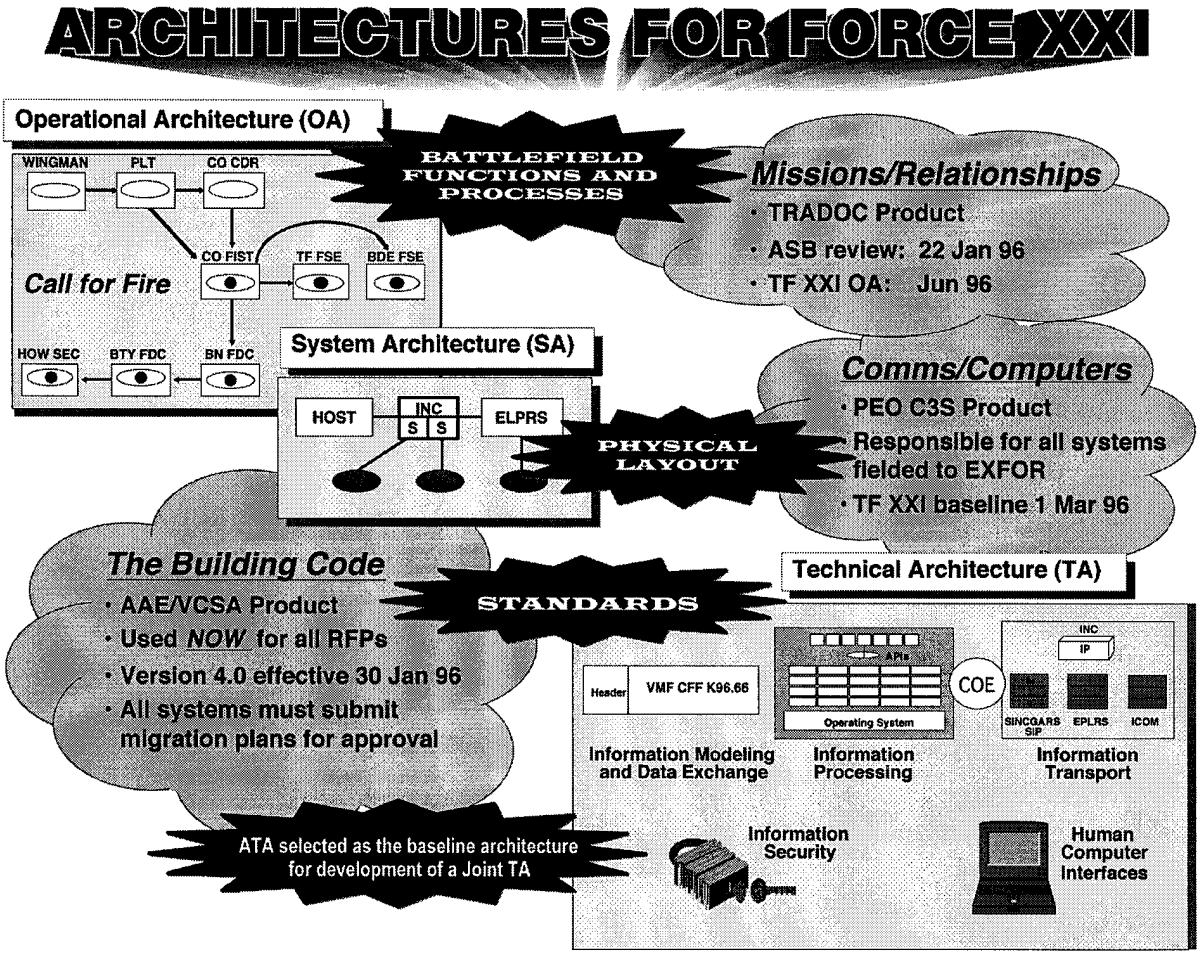


Figure 2. The Three Architectures

- **Technical Architecture (TA)** is the minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements that together may be used to form an information system. Its purpose is to ensure that a conformant system satisfies a specified set of requirements. It is the building code for the system architecture. The AAE is the Army's Technical Architect.

THE GLOBAL COMMAND AND CONTROL SYSTEM (GCCS)

The Department of Defense is migrating its command and control systems towards the common environment of the GCCS to provide the warfighter with a single integrated picture of the surrounding battlespace. Positioned at the upper levels of the joint command and control structure, GCCS provides the seamless, integrated information interface to manage and execute crisis and contingency operations. GCCS is the single command and control system for joint operations, and interfaces with the Army Battle Command System (ABCS). A Defense Information Infrastructure (DII) COE was recently established which will encompass both the GCCS and the Global Combat Support System (GCSS) in a single, integrated COE.

ARMY BATTLE COMMAND SYSTEM (ABCS)

The ABCS integrates Army battlespace systems and communications to functionally link strategic, operational, and tactical headquarters. ABCS components are:

- **Army Global Command and Control System (AGCCS),** which is the Army GCCS component system located at strategic and theater levels. It will be interoperable with other theater, joint, and multinational command and control systems, as well as with Army command and control systems at corps and echelons below corps.

- **Army Tactical Command and Control System (ATCCS)**, which will migrate to the DII COE and meet the command and control needs from brigade to corps.

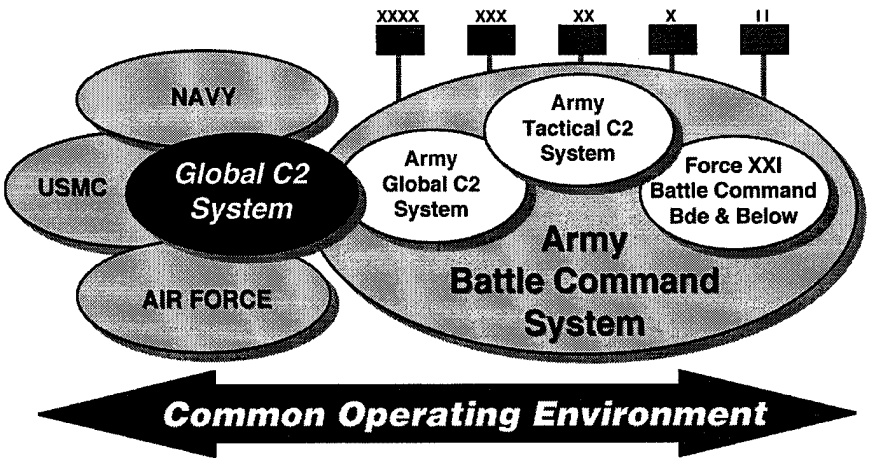


Figure 3. Army Battle Command System

- **Force XXI Battle Command Brigade-and-Below System (FBCB2),** which provides command and control needs below brigade–level and will also be COE–compliant.

IMPLEMENTATION STRATEGY

The execution of the Army digitization effort will be conducted in four major thrusts:

- Develop command and control software and applique hardware initially focused at brigade-and-below levels.
- Establish a seamless communication infrastructure—the *Tactical Internet*—which will evolve into an enhanced Warfighter Information Network (WIN).
- Integrate future digitally embedded weapons systems and non-embedded legacy systems into the *Tactical Internet* by means of standardized protocols, data standards, and message exchange formats, incorporating FBCB2 functionality where applicable.
- Develop a Battlefield Information Transmission System (BITS) that will augment the near-term implementation of the *Tactical Internet* with emerging commercially-based technologies that in the far–term will allow for the increased information flow necessary to support a fully digitized force.

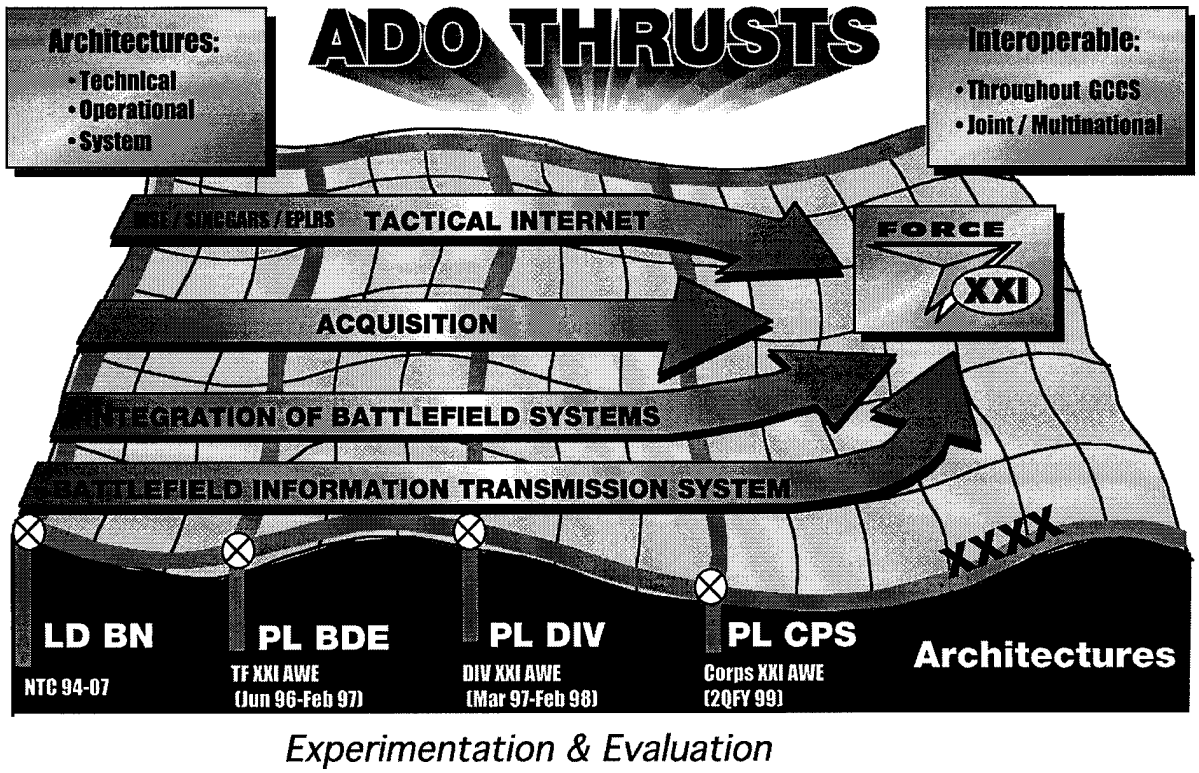


Figure 4. Digitization Axes, Phase Lines, and Objective

ACQUISITION STRATEGY

The primary goal of the acquisition strategy is to minimize the time and cost of satisfying Force XXI digitization requirements, consistent with basic DoD policies, sound business practices, available funding, and common sense. The strategy will be tailored to meet the specific needs of the Army digitization program and the evolving streamlined acquisition process. The intent of the strategy is to use a variety of contract types to accommodate the diversity of efforts required.

The approach adopted by the ADO involves four basic means for digitizing current and future platforms:

- Applying a digitized applique to current non-digitized platforms.
- Assuring that the communications capabilities of newly-acquired systems are compatible with the *Tactical Internet.*
- Inserting common software into existing/future embedded digital subsystems.
- Anticipating growth requirements and upgrades based on technology enhancements.

The acquisition strategy will be event-driven, with developmental efforts divided into three phases to avoid premature commitment to emerging technologies:

- **Phase 1: Concept Exploration (FY94-97).** This phase is oriented on defining and meeting the digitized requirements of the designated Experimental Force (EXFOR) in support of the Task Force XXI AWE, culminating in an exercise at the National Training Center (NTC). Following completion of the brigade-level AWE, a division-level AWE will be conducted, using a Battle Command Training Program (BCTP)–type Command Post Exercise (CPX) format. Phase 1 will terminate with a Milestone I/II Decision.
- **Phase 2: Demonstration (FY97-99).** Elements of the EXFOR will be upgraded with improved applique systems and a Force Development Test and Experimentation (FDTE) will be conducted. This will be followed by an Initial Operational Test and Evaluation (IOTE) to validate and verify changes recommended as a result of analysis following the FDTE, and to ensure that Critical Operational Issues and Criteria (COIC) have been met. After successful completion of the IOTE, Phase 2 will terminate with a Milestone III Decision.
- **Phase 3: Deployment (FY00-TBD).** Following the Milestone III review, a production contract will be competitively awarded, with follow-on fielding of Army XXI units.

ASSESSMENT STRATEGY

The Army has designed an iterative, building-block series of AWEs, modeling initiatives, and multi-level simulations to demonstrate discrete changes in force effectiveness as a result of fielding information technologies. Initial emphasis will be placed on the brigade-and -below piece of the future Army XXI.

Each experiment is structured around a *rolling baseline* concept that integrates experimentation, modeling, and simulation efforts. This rolling baseline uses cumulative data from relevant preceding experiments and exercises as the baseline for the next exercise.

Experiments offer many data collection opportunities to meet evaluation and assessment requirements. They will be designed and executed with the test and evaluation community (e.g., OPTEC, AMSAA, Electronics Proving Ground (EPG) and others) on-board from the beginning, so that the scope and level of dedicated testing and evaluation subsequently required to support procurement and fielding decisions is minimized. System performance data collection during train-up and exercises will be conducted so as to minimize interference with training and realism.

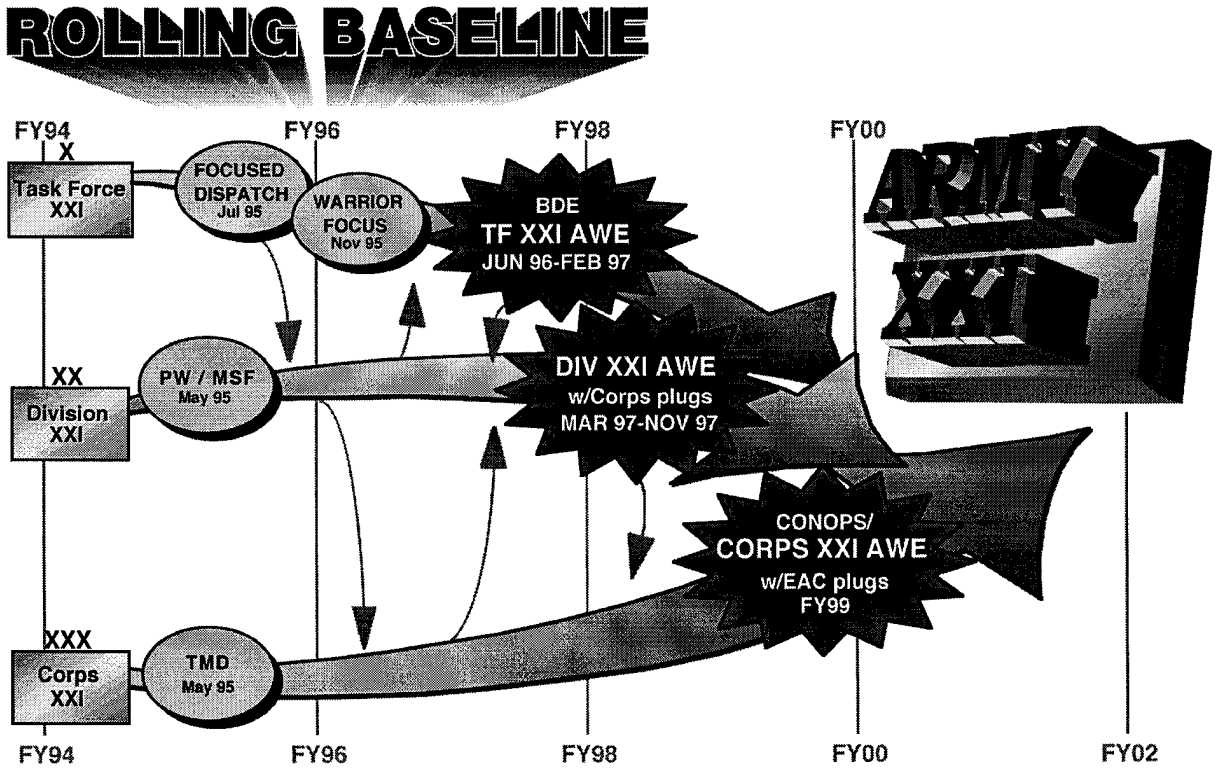


Figure 5. Experimentation Process

INFORMATION SYSTEMS SECURITY AND SURVIVABILITY

Digitization systems must operate at an appropriate level of security. This will be accomplished by integrating computer and communications security capabilities using technologies currently available. The three architectures provide the framework for security implementation:

- System architecture depicts implementation of security devices.
- Operational architecture addresses security requirements and associated tactics, techniques, and procedures (TTP).
- Technical architecture integrates security-related protocols and standards.

To properly manage ongoing actions necessary for information security within the digitized battlespace, the overall security effort is divided into four general activities:

- Policy and regulations are being modified to accommodate digital systems in a fast-moving tactical environment in which information is extremely time-sensitive.
- Revised TTP and training are being developed as a means of offsetting the need for security measures that may be too costly or not currently available.
- Military and commercial security technologies are being explored for subsequent integration into the Army's System and Technical Architectures.
- Vulnerability assessments are being conducted to assess weaknesses of current security systems and the ability of new security concepts to accomplish their intended purposes.

JOINT AND MULTINATIONAL INTEROPERABILITY

Joint and multinational interoperability is a continuous thread running through the entire fabric of the Army digitization effort. Established fora, such as the Military Communications-Electronics Board (MCEB) along with newly created structures—such as the Joint Battlefield Digitization Council of Colonels/Captains and the Joint Battlefield Digitization General Officer Working Group—are used to manage and integrate the Services' digitization efforts.

Bilateral Memoranda of Agreement between the Army and each of the other Services have been signed. All have agreed to participate in the major AWEs, provide input to the *Army Digitization Master Plan*, and conduct experiments to improve digital interoperability.

The goal in multinational cooperation is to establish and implement a basic strategy supporting coalition warfare through an increased level of digital interoperability. The objectives of multinational cooperation are outlined in the independently published *International Digitization Strategy*, which identifies and describes the priorities and processes that enhance the interoperability of the U.S. and its current/potential multinational partners. Success in all operational environments requires the harmonization of national doctrines, tactics, and techniques in support of coalition warfare and the development of cooperative technologies and standards to enable a truly seamless architecture. These objectives and goals are being accomplished by

meeting and overcoming the challenges of separate doctrine, varying degrees of automation, differences in technology, communication systems interoperability, financial variance between nations, political and economic disparities, and issues of security.

SUMMARY

The objective of the ADO and all the organizations involved in making Army XXI a reality is to create a force that will evolve into the Army of the 21st Century—equipped to face any contingency throughout the world; to win the information war against any adversary; and to provide deciders, shooters, and supporters the information each needs to make the myriad of vital decisions necessary to prevail in any future campaign.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

List of Acronyms and Abbreviations

A	
A2C2S	Army Airborne Command and Control System
AAE	Army Acquisition Executive
AAV	Amphibious Assault Vehicle
AAVP-7	Amphibious Assault Vehicle (Command Post Support Configuration)
AAWG	Army Armaments Working Group
ABCA	American, British, Canadian, Australian
ABCS	Army Battle Command System
ACE	Analysis and Control Element (Army)
ACE	Air Combat Element (Marine Corps)
ACT II	Advanced Concepts and Technology II
ACTD	Advanced Concepts Technology Demonstration
ADDS	Army Data Distribution System
ADMP	Army Digitization Master Plan
ADO	Army Digitization Office
ADSIA	Allied Data Systems Interoperability Agency
ADTOC	Air Defense Tactical Operations Center
AEPG	Analysis and Experimentation Planning Group
AFATDS	Advanced Field Artillery Tactical Data System
AF/SCM	Air Staff - Directorate of Mission Systems, DCS/C4
AF/XOR	Air Staff - Directorate of Operational Requirements, DCS/Plans & Operations
AGCCS	Army Global Command and Control System
AIN	Army Interoperability Network
AMC	Army Materiel Command
AMD	Air and Missile Defense
AMSAA	Army Materiel Systems Analysis Activity
ANBACIS	Automated Nuclear, Biological, Chemical Information System
ANM	Automatic Network Manager
API	Application Program Interfaces
AQF	Advanced Quickfix
ARL	Army Research Laboratory
ARPA	Advanced Research Projects Agency
ARSTAF	Army Staff
ARTEP	Army Training and Evaluation Program
ASA(RDA)	Assistant Secretary of the Army for Research, Development and Acquisition
ASAS	All Source Analysis System
ASAT	Automated Systems Approach to Training
ASB	Army Science Board

ASD C3I	Assistant SecDef for Command, Control, Communications, and Intelligence
ASEO	Army Systems Engineering Office
ASM	Armored Systems Modernization
ASWG	Army Battle Command System Security Working Group
ATA	Army Technical Architecture
ATCA	Allied Tactical Communications Agency
ATCCIS	Army Tactical Command and Control Information System
ATCCS	Army Tactical Command and Control System
ATD	Advanced Technology Demonstration
ATM	Asynchronous Transfer Mode
ATP	Allied Tactical Publication
AWE	Advanced Warfighting Experiment
AWIS	Army World Wide Military Command and Control System (WWMCCS) Information System

B

B2C2	Brigade-and-Below Command and Control
BAA	Broad Agency Announcement
BADD	Battlefield Awareness and Data Dissemination
BCBL	Battle Command Battle Lab
BCDSS	Battle Command Decision Support System
BCIS	Battlefield Combat Identification System
BCIXS	Battlecube Information Exchange System
BCTP	Battle Command Training Program
BDE	Brigade
BFA	Battlefield Functional Area
BFACS	Battlefield Functional Area Control Systems
BGP	Border Gateway Protocol
BIP	Battlefield Interoperability Program
BITS	Battlefield Information Transmission System
BLWE	Battle Lab Warfighting Experiments
BMDO	Ballistic Missile Defense Office
BOIP	Basis of Issue Plans
BOS	Battlefield Operating System
BSFV-E	Bradley Stinger Fighting Vehicle–Enhanced

C

C2	Command and Control
C2I	Command, Control, and Intelligence
C2PCOC	Command and Control Protect Council of Colonels
C2P GOSC	Command and Control Protect General Officer Steering Committee
C2PWG	Command and Control Protect Working Group
C2/SA	Command and Control/Situational Awareness
C2T2	Commercial Communications Technology Testbed

C2TL	Commercial Communication Technology Laboratory
C2V	Command and Control Vehicle
C3	Command, Control, and Communication
C3I	Command, Control, Communication, and Intelligence
C3S	Command, Control, and Communication Systems
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
C4IFTW	*C4I For the Warrior*
CA	Common Application
CAC2	Combined Arms Command and Control
CAE	Component Acquisition Executive
CBS	Corps and Battalion Simulation
CCC	CINC Command Complex
CDMA	Code Division Multiple Access
CDS	Combat Direction System
CE	Command Element
CECOM	Communications-Electronics Command
CERDEC	Communications-Electronics Command Research, Development, and Engineering Center
CEWG	Communications-Electronics Working Group
CGM	Computer Graphics Metafile
CGS/GSM	Common Ground Station / Ground Station Module
CHS	Common Hardware/Software
CINC	Commander-In-Chief
CLS	Contractor Logistics Support
CNR	Combat Net Radio
CoC	Council of Colonels
CoC/C	Council of Colonels/Captains
COE	Common Operating Environment
COIC	Critical Operational Issues and Criteria
COMSEC	Communications Security
CONOPS	Continuous Operations
CONUS	Continental United States
COTS	Commercial Off the Shelf
CPX	Command Post Exercise
CRDA	Cooperative Research and Development Agreements
CS	Combat Support
CSA	Chief of Staff, Army
CSS	Combat Service Support
CSSCS	Combat Service Support Control System
CSSE	Combat Service Support Element
CTC	Combat Training Center
CUI	Character User Interface
CWG	Communications Working Group

D

DAMO-ZS	Army Simulation Strategic Planning Office, DCSOPS, HQDA
DAMPL	Department of the Army Master Priority List
DBBL	Dismounted Battlespace Battle Lab
DBC	Digital Battlefield Communications
DCS	Defense Communications System
DCSINT	Deputy Chief of Staff for Intelligence
DCSLOG	Deputy Chief of Staff for Logistics
DCSOPS	Deputy Chief of Staff for Operations and Plans
DCSPER	Deputy Chief of Staff for Personnel
DCT	Digital Communications Terminal
DDDS	Defense Data Dictionary System
DGSA	Defense Goal Security Architecture
D/IEA	Data/Information Exchange Annex
DII	Defense Information Infrastructure
DIL	Digital Integrated Laboratory
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISC4	Director of Information Systems for Command, Control, Communications, and Computers
DISN	Defense Information System Network
DIV	Division
DMA	Defense Mapping Agency
DMS	Defense Message System
DoD	Department of Defense
DSB	Defense Science Board
DSSU	Dismounted Soldier System Unit
DTLOMS	Doctrine, Training, Leader Development, Organizations, Materiel, and Soldiers

E

EAC	Echelons Above Corps
EIM	End Item Managers
EMUT	Enhanced Manpack Ultra High Frequency (UHF) Terminals
EPG	Electronic Proving Ground
EPLRS	Enhanced Position Location Reporting System
EW	Electronic Warfare
EXFOR	Experimental Force
EXMP	Experimentation Master Plan

F

FAADC2I	Forward Area Air Defense Command, Control, and Intelligence

FBCB2	Force XXI Battle Command Brigade-and-Below
FDTE	Force Development Test and Evaluation
FIO	Force XXI Integration Office
FIPS	Federal Information Processing Standards
FLIR	Forward Looking Infra-Red
FMF	Fleet Marine Force
FORSCOM	Forces Command
FP-1	Force Package One
FSCT	Fire Support Control Terminal
FST	Fire Support Terminal
FTP	File Transfer Protocol
FUE	First Unit Equipped
FY	Fiscal Year

G

GBS	Global Broadcasting System or Ground Based Sensor (fig 9-1)
GBCS-LT	Ground Based Common Sensor–Light
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GCE	Ground Combat Element
GFI	Government Furnished Information
GLOBIXS	Global Information Exchange System
GOAL	Global Command and Control System (GCCS) On-Line Access Library
GOSC	General Officer Steering Committee
GOWG	General Officer Working Group
GPS	Global Positioning System
GUI	Graphical User Interface

H

HCI	Human Computer Interface
HCTR	High-Capacity Trunk Radio
HIBC	Horizontal Integration of Battle Command
HQDA	Headquarters, Department of the Army
HTI	Horizontal Technology Integration
HTML	HyperText Markup Language
HW	Hardware

I

IC2SIP	International Command and Control Systems Interoperability Project
IC3I	Improved Command, Control, Communications and Intelligence
ICD	Interface Control Document
ID	Identification
IDEF	Integrated Definition for Function
IDS	International Digitization Strategy

IER	Information Exchange Requirement
IEW	Intelligence and Electronic Warfare
IFB	Invitation for Bids
IFSAS	Interim Fire Support Automated System
ILS	Integrated Logistics Support
IMETS	Integrated Meteorological System
INC	Interface Network Controller
INE	Inline Network Encryptors
IOTE	Initial Operational Test and Evaluation
IP	Internet Protocol
IPR	In-Process Review
IPT	Integrated Product Team
I&RTS	Integration and Runtime Specification
ISYSCON	Integrated Systems Control
ITU	International Telecommunications Union
IVIS	Intervehicular Information System

J

JBD	Joint Battlefield Digitization
JC2WC	Joint Command and Control Warfare Center
JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability Engineering Organization
JINTACCS	Joint Interoperability Command and Control System
JITC	Joint Interoperability Test Center
JMCIS	Joint Maritime Command Information System
JOPES	Joint Operations Planning and Execution System
JROC	Joint Requirements Oversight Council
JTIDS	Joint Tactical Information Distribution System
JWID	Joint Warrior Interoperability Demonstration

K

Kr	Contractor

L

LAN	Local Area Network
LAV	Light Armored Vehicle
LIWA	Land Information Warfare Activity
LMR	Land Mobile Radio
LUT	Limited User Test
L/V/C	Live/Virtual/Constructive
LVRS	Lightweight Video Reconnaissance System

M

MA	Mission Application

MACOM	Major Command
MAGTF	Marine Air-Ground Task Force
MANPRINT	Manpower and Personnel Integration
MARCORSYSCOM	Marine Corps Systems Command
MASINT	Measurement & Signal Intelligence
MBBL	Mounted Battlespace Battle Lab
MCCDC	Marine Corps Combat Development Command
MCEB	Military Communications Electronic Board
MCG&I	Mapping, Charting, Geodetic Data and Imagery
MCS	Maneuver Control System
MCS/P	Maneuver Control System/PHOENIX
MDA	Milestone Decision Authority
MDCI	Multidiscipline Counter-Intelligence
MDEP	Management Decision Package
MEU	Marine Expeditionary Unit
MFCS	Mortar Fire Control System
MICAD	Multipurpose Integrated Chemical Agent Detector
MIL-STD	Military Standard
MISSI	Multi-level Information System Security Initiative
MITT	Mobile Imagery Tactical Terminal
MLS	Multi-level Security
MNS	Mission Need Statement
MOA	Memorandum (Memoranda) of Agreement
MOE	Measures of Effectiveness
MOP	Measures of Performance
MPRS	Mission Planning and Rehearsal System
M/S	Modeling and Simulation
MS	Milestone
MSE	Mobile Subscriber Equipment
MSE/TPN	Mobile Subscriber Equipment/Tactical Packet Network
MSF	Mobile Strike Force
MSIP	Multi-Spectral Imagery Processor
MSRT	Mobile Subscriber Radio Terminal

N

NAAG	NATO Army Armaments Group
NATO	North Atlantic Treaty Organization
NBC	Nuclear, Chemical, Biological
NDI	Non-Developmental Item
NES	Network Encryption System
NET	New Equipment Training
NITFS	National Imagery Transmission Format Standard
NSA	National Security Agency
NTC	National Training Center

NTDR	Near-Term Data Radio

O

O&M	Operations and Maintenance
OA	Operational Architecture
OPO	Operational Performance Objectives
OPSEC	Operational Security
OPTEC	Operational Test and Evaluation Command
ORA	Operational Requirements Analysis
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OSI	Open System Interconnection
OS-JTF	Open Systems Joint Task Force
OT	Operational Test
OTM	On-the-move

P

P3I	Pre-Planned Product Improvement
PAT	Process Action Team
PCS	Personal Communications System
PDA	Personal Digital Assistant
PE	Program Element
PEO	Program Executive Office
PG	Planning Group
PLGR	Position Location Ground Receiver
PLS	Palletized Loading System
PM	Program Manager
PND	Position-Navigation Device
POM	Program Objective Memorandum
POSNAV	Position/Navigation
POSIX	Portable Operating System Interface for Computer Environments
PPBES	Planning, Programming, Budgeting, and Execution System
PPP	Point-to-Point Protocol
PW/MSF	Prairie Warrior / Mobile Strike Force

Q

QACISIG	Quadrilateral Army Communications and Information Systems Interoperability Group

R

R&D	Research and Development

RAP	Radio Access Point
RAS	Rapid Assault Squads
RDEC	Research Development and Engineering Center
RDTE	Research, Development, Test, and Evaluation
RF	Radio Frequency
RFP	Request for Proposal
RMMP	Risk Management Master Plan
RT	Red Team

S

S&T	Science and Technology
SA	System Architecture
SADL	Situation Awareness Digital Link
SAF/AQP	Director of Fighter, Command and Control, and Weapon Programs; Office of the Deputy Assistant Secretary of the Air Force for Communications, Computer and Support Systems
SARDA	Assistant Secretary of the Army for Research, Development, and Acquisition
SAT	Systems Approach to Training
SATCOM	Satellite Communication
SATS	Standard Army Training System
SDR	Surrogate Data Radio
SEP	System Enhancement Program
SG	Subgroup
SHAPE	Supreme Headquarters Allied Powers Europe
SICPS	Standardized Integrated Command Post System
SIGCEN	Signal Center
SIMEX	Simulation Exercise
SIMNET	Simulation Network
SINCGARS	Single Channel Ground and Airborne Radio System
SIP	SINCGARS Improvement Program
SIPRNET	Secret Internet Protocol Network
SIPT	Security Integrated Product Team
SLAD	Survivability/Lethality Analysis Directorate
SNMP	Simple Network Management Protocol
SOF	Special Operating Forces
SONET	Synchronous Optical Network
SOW	Statement of Work
SPAWAR/30	Space and Naval Warfare Systems Command - Naval Warfare Systems Architecture & Engineering
SSDC	Space and Strategic Defense Command
SSES	Suite of Survivability Enhancement Systems
SSN	Standard Study Number
STAARS	Standard Army After Action Review System

STAMIS	Standard Army Management Information System
STAR-T	Super High Frequency Tri-Band Advanced Range Extension Terminal
STCCS	Strategic Theater Command and Control System
STEP	Standardized Tactical Entry Point
STF	Special Task Force
STIC	Scientific and Technical Intelligence Committee
STOW	Synthetic Theater of War
STRICOM	Simulations, Training, and Instrumentation Command

T

T&E	Test and Evaluation
TA	Technical Architecture
TAA	Total Army Analysis
TACCIMS	Theater Automated Command and Control System
TACOM	Tank-Automotive Command
TACP	Tactical Air Control Party
TADIL	Tactical Digital Information Link
TADIXS	Tactical Data Information Exchange System
TADSS	Training Aids, Devices, Simulators, and Simulations
TAFIM	Technical Architecture for Information Management
TCC	Tactical Command Centers
TCO	Tactical Command and Operations
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
TDA	Table of Distribution and Allowances
TDLWG	Tactical Data Link Working Group
TDN-EBB	Tactical Data Network-Echelons Below Battalion
TECOM	Test and Evaluation Command
TEED	Tactical End-to-End Encryption Device
TEMP	Test and Evaluation Master Plan
TF	Task Force
THAAD	Theater High Altitude Air Defense
TIDP	Technical Interface Design Plan
TIWG	Test Integration Working Group
TMD	Theater Missile Defense
TMG	Tactical Multinet Gateway
TO&E	Tables of Organization and Equipment
TOC	Tactical Operations Center
TPN	Tactical Packet Network
TRAC	Training and Doctrine Command Analysis Center
TRADOC	Training and Doctrine Command
TRITAC	Tri-Service Tactical
TRM	Technical Reference Model

TS3	Top Secret Support System
TSARC	Test Schedule and Review Committee
TSGCE	Technology Sub-Group: Communications and Electronics
TSIP	Task Force XXI Systems Integration Plan
TT	Technical Test
TTCP	The Technology Cooperative Program
TTP	Tactics, Techniques, and Procedures
TWG	Technology Working Group

U

UAV	Unmanned Aerial Vehicle
UAV-SR	Unmanned Aerial Vehicle–Short Range
UDP	User Datagram Protocol
UFD	User Functional Description
USAEUR	U.S. Army Europe
USANCA	U.S. Army Nuclear Chemical Agency
USMTF	U.S. Message Text Format

V

VCSA	Vice Chief of Staff, Army
VHSIC	Very High Speed Integrated Circuit
VMF	Variable Message Format

W

WAN	Wide Area Network
WG	Working Group
WIN	Warfighter Information Network
WS	Work Station
WSTA	Weapons System Technical Architecture
WWMCCS	Army World Wide Military Command and Control System

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

DEFINITIONS

Advanced Concept Technology Demonstrations	Advanced Concept Technology Demonstrations (ACTDs) allow the user to gain understanding and perform an evaluation of a military utility before committing to acquisition; development of corresponding operational and doctrinal concepts; and providing operational capabilities to the force.
Advanced Field Artillery Tactical Data System	Advanced Field Artillery Tactical Data System (AFATDS) is an integrated fire support command and control system that will process mission and other related information to coordinate and maximize the use of all fire support assets. AFATDS will provide processing capabilities from Corps to the Platoon Fire Direction Center.
Advanced Technology Demonstration	Advanced Technology Demonstrations (ATDs) are large-scale in resources and complexity; operator/user involved from planning to final documentation; tested in a real and/or synthetic operational environment typically five years or less; and cost schedule, and performance baselined.
Advanced Warfighting Experiment	Major event conducted in a tactically rigorous environment to confirm experimental hypotheses regarding increases in warfighting capability. System performance data collection during these events will be limited to minimize interference with training, realism, and other objectives.
All Source Analysis System	All Source Analysis System (ASAS) is a ground-based automated intelligence processing and dissemination system designed to provide intelligence and targeting support to the battle commanders.
Applique	The Applique is the Force XXI Battle Command Brigade-and-Below (FBCB2) initiative to digitize the battlefield. Computer hardware, software and interfaces will be installed on weapons platforms and vehicles at brigade–and–below echelons and deployed with individual dismounted soldiers.
Applique Hardware	The four versions of the Applique are: Commercial (V1), Ruggedized (V2), Militarized (V3), and Dismounted Soldier System Unit (DSSU)
Applique Installation Kits	Installation kits will be developed to accommodate installation of designated versions of applique hardware on the host platforms. Installation kits for applique hardware will vary by host platform.
Applique	The core of common application software functionality is the command and

Software control portion of the Intervehicular Information System Command and Control (IVIS C2) software and the Brigade-and-Below Command and Control (B2C2) software. The core of the common *support* software is a tailored subset of the Common Operating Environment (COE).

Army Battle Command System Army Battle Command System (ABCS) will be a combination of all migrated Army Command and Control Systems. The ABCS will include Army Global Command and Control System (AGCCS), Army Tactical Command and Control System (ATCCS), and Force XXI Battle Command Brigade-and-Below (FBCB2). It will employ a mix of fixed/semi-fixed installations and mobile networks and will be interoperable with theater, joint, and combined command and control systems.

Army Global Command and Control system Army Global Command and Control System (AGCCS) is the Army component of the Joint Global Command and Control System (GCCS). AGCCS will be built from application programs developed by the Army World Wide Military Command and Control system (WWMCCS) Information System (AWIS), the Standard Theater Command and Control System (STCCS), and the Echelon Above Corps (EAC) portion of the Combat Service Support Control System (CSSCS)

Army Tactical Command and Control System Army Tactical Command and Control System (ATCCS) is made up of five systems: Maneuver Control System (MCS); Forward Area Air Defense Command Control and Intelligence System (FAADC2I); All Source Analysis System (ASAS); Combat Service Support Control System (CSSCS); and Advanced Field Artillery Tactical Data System (AFATDS). ATCCS will be linked directly to Army Global Command and Control System (AGCCS), providing a framework of seamless connectivity from brigade to corps. ATCCS is also the linchpin between AGCCS and Force XXI Battle Command Brigade-and-Below (FBCB2), creating a holistic, seamless integration of battle command from individual platforms to echelons above corps (EAC).

Army WWMCCS Information System The Army WWMCCS Information System (AWIS) fulfills the Army's strategic command and control requirement for software, hardware, and databases for the implementation of the Joint Operations Planning and Execution System (JOPES) and other Joint/Service systems that support the CINCs and Joint Chiefs of Staff.

Battle Lab Warfighting Experiments Battle Lab Warfighting Experiments (BLWEs) are virtual, constructive, or live field events to examine new equipment, processes, and force design issues. BLWEs should provide significant opportunities for rigorous data collection to satisfy evaluation requirements.

Battle Labs TRADOC has six Battle Labs to identify, develop, and experiment with new

warfighting concepts and capabilities offered by emerging technologies. The Battle Lab concept is designed to provide hands-on user involvement during the early part of the requirements and acquisition process. This early involvement is expected to produce better requirements definitions during the research and advanced technology stages of programs, when decisions that determine most of the system's life cycle costs are made.

Battlefield Information Transmission System — Battlefield Information Transmission System (BITS) is a program developing commercial technologies which will allow much larger information throughput for the *Tactical Internet.*

Battlefield Operating System — The Battlefield Operating Systems (BOSs) are the major functions performed by the force on the battlefield to successfully execute Army operations (battles and engagements) in order to accomplish military objectives directed by the operational commander. They include maneuver, fire support, air defense, command and control, intelligence, mobility and survivability, and combat service support.

Battlefield Visualization — Battlefield Visualization is the process whereby the commander/soldier develops a clear understanding of the current state with relation to the enemy and the environment; envisions a desired outcome; and subsequently visualizes the sequence of activity that will move the force from its current state to the end state.

Brigade-and-Below Command and Control System — Brigade-and-Below Command and Control (B2C2) is a prototype suite of digitally interoperable BOS specific functional applications designed to provide near-real-time situational information to tactical commanders, on the move, down to platform/squad level.

Combat Service Support Control System — Combat Service Support Control System (CSSCS) will consolidate and collate the data required to integrate situational awareness of the combat service support mission areas. CSSCS will provide strategic and tactical commanders with information on ammunition and fuel supplies, medical and personnel status, transportation, maintenance services, general supply, and other field services.

Common Operating Environment — The Common Operating Environment (COE) is a set of integrated services supporting mission application software requirements. It also provides a corresponding software development environment, architecture principles, and methodology assisting in development of mission application software.

Copernicus — The Navy and Marine Corps definition of the *C4I for the Warrior* describing the establishment of an Information Warfare strategy and capability.

Digital Integrated Laboratory	The Digital Integrated Lab (DIL) is run by the U.S. Army Communications-Electronics Command (CECOM) Research, Development and Engineering Center (CERDEC) at Fort Monmouth, New Jersey. The DIL is used to develop, maintain, improve, and certify interoperability between and among Command, Control, Communications, Computers and Intelligence (C4I) and Electronic Warfare (EW) hardware and software prior to participating in the Task Force XXI experiment and follow-on AWEs. Use of the DIL is encouraged within and between systems being developed, systems already fielded, and science and technology programs.
Digitization	Digitization is the application of technologies to acquire, exchange, and employ timely digital information throughout the battlespace, tailored to the needs of each *decider* (commander), *shooter*, and *supporter*. Digitization allows each soldier to maintain a clear and accurate vision of the common battlespace necessary to support planning and execution.
Digital Integrated Lab Certification	Digital Integrated Laboratory (DIL) certification assures the Army Digitization Office (ADO) that the interoperability problems that arise from developing software into systems of Force XXI have been identified and resolved prior to the field exercises and experiments. DIL certification does not eliminate or replace any Army acquisition requirements.
Embedded Systems	Embedded systems are platforms with digital system components providing functions and processes which are integrated to such an extent that they cannot be considered as discrete entities during development, testing, or production of the system.
Enterprise Strategy	The *Enterprise Strategy* is the synchronization of Army programs with the Joint Staff's *C4I for the Warrior* concept; sound business practices; and *Defense Information Infrastructure Master Plan.*
Experimentation Force (EXFOR)	Elements of the reflagged 4th Infantry Division (Mechanized)—previously the 2nd Armored Division—which will be equipped with the most modern digital equipment in the Army in order to assess Force XXI concepts.
Force XXI Battle Command Brigade-and-Below	As a subset of Army Battle Command System (ABCS), Force XXI Battle Command Brigade-and-Below (FBCB2) provides an integrated command and control system that extends horizontally across all Battlefield Operating Systems (BOS) and vertically from individual squad/platform to brigade/regimental headquarters. It also provides a seamless, holistic battle command capability to leaders of all combat, combat support, and combat service support units performing missions at the tactical level of operations.
Forward Area Air Defense	Forward Area Air Defense (FAAD) is an integrated system of weapons, sensors, and Command, Control, and Intelligence (C2I). It protects maneuver

Command, Control, and Intelligence	forces, critical command posts, and combat support and combat service support elements from low–altitude air attack. FAADC2I is the element that provides air defense C2 and targeting information to weapons systems at the division–level.
Global Command and Control System	Global Command and Control System (GCCS) is a collection of broadly connected joint systems that provide total battlespace information to the warrior.
Horizon	*Horizon* is the Air Force vision for implementing *C4I for the Warrior.*
Horizontal Technology Integration	Horizontal Technology Integration (HTI) is the management process by which the Army takes an evolving technology breakthrough and maximizes its value by applying the capability across the spectrum of systems that need it, thereby obviating the need for independent and high cost development of similar functionalities.
Maneuver Control System	Maneuver Control System (MCS) provides commanders with the capability to collect, coordinate, and act on near-real-time battlefield information.
Multinational Operations	Military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance.
Non-Developmental Items	Deliverable items not developed under the contract but provided by the contractor, the Government, or a third party. Non-Developmental Items (NDI) may be referred to as reusable, Government furnished, or commonly available software, hardware, or total system, depending upon the source.
Operational Architecture	Operational Architecture (OA) establishes the basic framework and structure for what is to be built. An Operational Architecture defines the field deployment of the system components to the force by echelon, unit type, equipment, and information exchange requirements. It describes—typically graphically—who needs to exchange information, what information needs to be exchanged, and how that information will be used. It also addresses the platforms and equipment that are to be available, as well as the methodology to upgrade and interoperate with platforms containing embedded processors.
Operational Test	Event conducted to obtain data on total system performance when employed by representative soldiers in an operational environment. Operational Tests (OT) are conducted as necessary to fill *data voids* in order to provide credible operation assessments for procurement and fielding decisions.
Sea Dragon	The Marine Corps' concept for a 21st century firepower-based doctrine using small independent units equipped with improved targeting and digital C2 to

	saturate the battlefield and employ supporting artillery and aerial assets to disrupt and destroy the enemy.
Standard Theater Command and Control System	The Standard Theater Command and Control System (STCCS) is primarily designed to assist a theater commander in the execution of crisis and wartime sustainment and operational maneuver functions at echelons above corps (EAC)
Stovepipe Systems	Systems or platforms developed to perform specific functions, but not designed to be interoperable with other non-related platforms or systems.
System Architecture	The System Architecture (SA) is the technical companion document to the Operational Architecture. It establishes the specific hardware needed to provide the connectivity required in the Operational Architecture. The System Architecture is a description of the physical connectivity of an information system which includes: identification of all equipment and their physical deployment; the specification of such parameters as the bandwidth required on each circuit; and the description—including graphics—of technical characteristics and interconnection of all parts of an information system.
Situational Awareness	Knowledge of one's location; the location of friendly and hostile forces; and of external factors, such as terrain, weather, etc., that may affect one's capability to perform a mission.
Tactical Internet	The *Tactical Internet* is the integrated battlefield communications network. This network will provide reliable, seamless and secure communications connectivity required to support the applique, other command and control systems, and embedded systems. Information flow within the network is based on the exchange of Variable Message Format (VMF) messages using the commercially based Internet Protocol (IP).
Technical Architecture	The Technical Architecture (TA) is defined as a minimal set of rules governing the arrangement, interaction, and interdependence of the parts of an information system. The purpose of the Technical Architecture is to ensure that a conformant system satisfies a specific set of requirements.
Technical Architecture Framework for Information Management	Technical Architecture Framework for Information Management (TAFIM) is a set of Joint standards, design concepts, components, and configurations that can be used to guide the development of the Service's technical architectures that meet specific mission requirements.
Variable Message Format	Variable Message Format (VMF) provides a common set of messages in a standard format that can be used by the tactical data systems of all services or agencies to achieve full joint interoperability.

Vertical Technology Integration	The process of maximizing the value of a new technology by applying it vertically from the lowest level of operations to the highest level of command to provide a common understanding throughout the command.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

REFERENCES

Advanced Warfighting Experiment Focused Dispatch Battle Lab Experiment Plan (Draft), dated 16 Feb 95

Army Technical Architecture, Version 4.0, dated 30 Jan 96

Army Digitization Acquisition Strategy, dated 30 Nov 94

Army Digitization Master Plan 95, dated 30 Jan 95

Army Digitization Office Campaign Plan, dated 17 Nov 94

Army Digitization Office Charter, dated 9 Jun 94.

Army Digitization Office Resources for Master Plan (Funding)

Army Digitization Office Risk Management Master Plan

Army Enterprise Implementation Plan, dated 8 Aug 94

Army Enterprise Strategy, The Vision, dated 20 Jul 93

Army Experimentation Master Plan (EXMP) for Force XXI Battle Command Brigade-and-Below (FBCB2), Revision A, dated 28 Jun 95

Battlefield Information Transmission System Far-Term Strategy (version 1.0), dated 1 Oct 95.

Battle Labs, Force XXI, Defining the Future, dated May 95

Defense Information Infrastructure Integration and Run time Specification: Rev 2.0, dated 23 Oct 95

EXFOR Advanced Warfighting Experiment (AWE) Initiatives, updated monthly.

Fire Support Digitization Master Plan (FSDMP) Draft, dated 4 Aug 95.

Horizon, Air Force C4I Strategy for the 21st Century

International Digitization Strategy, Army Materiel Command, dated 1 Mar 96

JP 1 (*Joint Warfare for the Armed Forces*), dated 11 Nov 91.

JP 3.0 (*Doctrine for Joint Operations*), dated 9 Sep 93.

Memorandum of Agreement between the Department of the Army and the Department of the Navy; Subject: US Army, US Navy, and US Marine Corps Battlefield Battlespace Digitization Coordination, dated 21 Feb 95.

Memorandum of Agreement between the Department of the Army and the Department of the Air Force; Subject: US Army and US Air Force Battlefield/Battlespace Digitization Coordination, dated 22 Jul 95.

Amendment One (International C2 Systems Interoperability Program) to the Memorandum of Understanding between the Secretary of Defense of the United States of America and the Federal Minister of Defense of the Federal Republic of Germany Concerning the Joint Research, Development, and Demonstration off a Combat Vehicle Command and Control System.

Memorandum for Program Executive Officer; Command, Control, and Communications, regarding Applique Hardware Requirements, dated 17 Jun 95, from MG Joe W. Rigby, Director, Army Digitization Office.

Memorandum for Multiple Addressees, regarding Digitization Rules, dated 8 Mar 95, from zy Joe W. Rigby, Director, Army Digitization Office.

Memorandum for Multiple Addressees, regarding Digitization Programs Input for the FY98-03 POM and FY98-12 RDA Plan, dated 12 Feb 96, from MG Joe W. Rigby, Director, Army Digitization Office.

Mission Need Statement for Horizontal Integration of Battle Command (HIBC), dated 7 Mar 95

NCSC-TG-003 (*A Guide to Understanding Discretionary Access Control in Trusted Systems*), dated 30 Sep 87.

Security Classification Guide for the Army Digitization Initiative (Draft), dated 30 Oct 95.

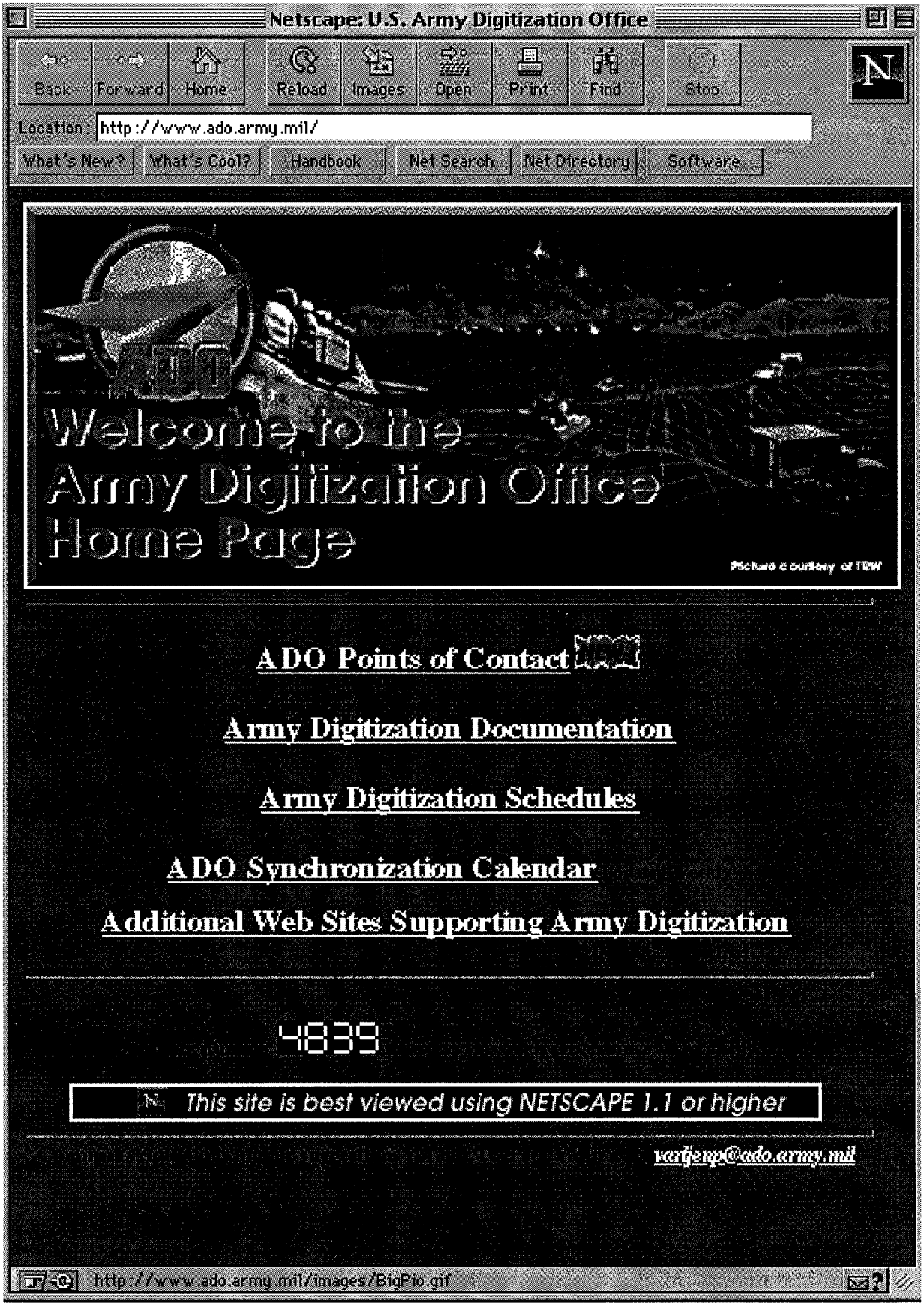
SOF Master Plan (Draft), undated.

Task Force XXI Information Systems Red Team Plan (Draft), dated 30 Oct 95.

Task Force XXI Systems Integration Plan (Draft), dated 25 Oct 95.

Warrior Focus JRTC-96-02, Battle Lab Exercise Directive, dated 21 Feb 95

Copies of all reference material can be obtained from the ADO at the address on page C-4; at phone number (703) 693-3412 or DSN 223-3412; or on the ADO Home Page on the World Wide Web (http://www.ado.army.mil).


Netscape: U.S. Army Digitization Office
Back
Forward
Home
Reload
Images
Open
Print
Find
Stop
Location: http://www.ado.army.mil/
What's New?
What's Cool?
Handbook
Net Search
Net Directory
Software
Welcome to the Army Digitization Office Home Page
Picture courtesy of TRW
ADO Points of Contact
Army Digitization Documentation
Army Digitization Schedules
ADO Synchronization Calendar
Additional Web Sites Supporting Army Digitization
4839
This site is best viewed using NETSCAPE 1.1 or higher
varjenp@ado.army.mil
http://www.ado.army.mil/images/BigPic.gif

ARMY DIGITIZATION OFFICE
DACS-ADO
Office of the Chief of Staff, Army
200 ARMY PENTAGON
WASHINGTON DC 20310-0200

APPENDIX D

ADO POINTS OF CONTACT

(AS OF 03/96)

ADDRESS: ARMY DIGITIZATION OFFICE
DACS-ADO
OFFICE OF THE CHIEF OF STAFF, ARMY
200 ARMY PENTAGON
WASHINGTON, D.C. 20310-0200

AUTODIN ADDRESS: HQDA WASHINGTON DC//DACS-ADO//

TELEPHONE PREFIXES: Commercial - Area Code (703) + 7 digits
DSN - 223 + last 4 digits

INTERNET HOME PAGE IP ADDRESS: http://ado.army.mil

Organization	POC	Room #	Phone	EMail
Army Digitization Office Headquarters				
Director	MG Rigby	2B679	693-3300	rigbyr@ado.army.mil
Deputy Director	Mr. White	2B679	693-3302	whited@ado.army.mil
Executive Officer	LTC Singleton	2B679	693-3302	singlw@ado.army.miL
Fax			693-4100	
Acquistion Team				
Chief	COL Langford	2B683	693-3415	langforw@ado.army.mil
Programs/COR	Ms. Barber	2B683	693-3399	barbere@ado.army.mil
Budget	Mr. Cook	2B683	693-3297	cooks@ado.army.mil
Programs	Mr. Grohman	2B683	693-3372	grohmans@ado.army.mil
Programs/COR	LTC Jones	2B683	693-3298	jonesl@ado.army.mil
Business Manager	Ms. Munday	2B683	693-3437	mundayj@ado.army.mil
Budget	Ms. Queen	2B683	693-3427	queenp@ado.army.mil
Fax			693-3400	
Architecture Team				
Chief	COL Fornecker	1D640	693-3728	forneckc@ado.army.mil
Security	Mr. Allen	Crystal City	413-3200	allenh@ado.army.mil
Systems	Mr. Balough	1D640	693-3887	baloughm@ado.army.mil
GCCS/18820 Standards	Ms. Bhagowalia	1D640	693-3620	bhagowad@ado.army.mil
Armored Systems	Mr Rager	1D640	693-3616	ragers@ado.army.mil
Software Architecture	LTC Skertic	1D640	693-3509	skerticr@ado.army.mil
Fax			693-4101	

Integration Team

Chief	COL Langford	2B683	693-3415	langforw@ado.army.mil
Graphics	Mr. Ayers	2B683	693-3391	ayersr@ado.army.mil
Presentations	Mr. Butler	2B683	693-3368	butlerj@ado.army.mil
Joint/International	LTC Cox	2B683	693-3411	coxs@ado.army.mil
Scheduling/Issues	Mr. Derks	2B683	693-3410	derksl@ado.army.mil
Aviation/Battlefield Vis	Mr. Ferrell	2B683	693-3414	ferrelld@ado.army.mil
Risk Management	Mr VanHoose	2B638	693-3370	vanhoose@ado.army.mil
Army Integration/Synchron.	LTC Varljen	2B683	693-3412	varljenp@ado.army.mil
Fax			693-3400	

Requirements and Evaluation Team

Chief	COL Emison	1A869	693-3773	emisons@ado.army.mil
Safety	Mr. Briski	Ft. Meade(301)	677-2178	*no mil net address*
Requirements	Mr. Cross	1A869	693-3861	crossr@ado.army.mil
Testing	Mr. Gates	1A869	693-3893	gatess@ado.army.mil
Simulation	Ms. Wright	1A869	693-3856	wrights@ado.army.mil
Exercise Force (EXFOR)	MAJ Reaves	1A869	693-3863	reavess@ado.army.mil
Fax			693-4102	

TABLE OF CONTENTS

APPENDICES

FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK